UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

RACHELLE RAND, ESPERANZA GOTTSCHAU, RAMON SOTO, GEORGIANNA LASH, and AARON MEES on Behalf of Themselves and All Others Similarly Situated, Plaintiffs, v. EYEMART EXPRESS, LLC, Defendant.	**Case No.: 3:24-cv-00621-N** **AMENDED CLASS ACTION COMPLAINT** **<u>DEMAND FOR JURY TRIAL</u>**

Plaintiffs Rachelle Rand, Esperanza Gottschau, Ramon Soto, Georgianna Lash, and Aaron Mees (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, by and through their undersigned counsel, bring this class action complaint against Defendant Eyemart Express, LLC (the "Defendant" or "Eyemart"). Plaintiffs allege the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiffs, which are alleged upon personal knowledge.

NATURE OF THE ACTION

1. Eyemart Express controls and operates https://eyemartexpress.com/ (the "Website" or "Eyemart Website"). On the Website, users browse health-related eye products (the "Browsers"), purchase prescription eyewear (the "Purchasers") and locate a doctor to schedule eye examinations (the "Examinees") (the Browsers, Purchasers, and Examinees are collectively referred to as the "Tracked Users"). The Website offers the option for Tracked Users to search for prescription eyewear products, which can then be purchased online or from local Eyemart store

locations, and the Website offers various methods to connect to a local Eyemart store to schedule an eye exam.

2. To use the Website's search function (the "Search Bar"), Tracked Users type search queries or search terms (the "Queries") into the Search Bar. The Search Bar is used to search for specific goods on the Website. After typing and submitting Queries into the Search Bar, results are obtained from the Website and displayed as a list to its Tracked Users.

3. To schedule eye exams with eye specialists, Tracked Users may use the Website to search for physical Eyemart locations based on geographical location. Once a store is selected, the Website provides various methods to schedule eye exams, including online scheduling, phone numbers to call the locations, and addresses to visit the locations.

4. Unbeknownst to Tracked Users, Eyemart employs tracking tools on the Website which intercept communications between Tracked Users and the Website.

5. Meta's Pixel (the "Pixel" or "Facebook Pixel" or "Meta Pixel") is a tracking tool which was created by Meta (also referred to as "Facebook" or the "Tracking Entity") to send the Tracking Entity information relating to Tracked Users' searches and activity on any website that installed it, including the Eyemart Website.

6. Further, when Tracked Users click to find specific items on the Website or purchase prescription eyewear, a description of each item is sent to the Tracking Entity (such as make, model, materials, and product ID of frames and lenses), in addition to details about Tracked Users' attempts to schedule eye exams (collectively, the "Personal Health Information" or "PHI").

7. The Website does not provide Tracked Users with notice that the Website's use of a Search Bar would cause their Queries to be intercepted by the Tracking Entity, that viewing items will result in information about those items being intercepted by the Tracking Entity, that attempts to schedule eye exams will result in information related to the eye exam being intercepted,

or that such interceptions will be used to benefit the Defendant and Tracking Entity separate from the services being rendered to the Tracked User.[1]

8. Importantly, Eyemart does not obtain Tracked Users' consent to its disclosure practices prior to Tracked Users' use of the Website.

9. Tracking tools, such as the Meta Pixel, improve the value of advertising sold on to websites and purchased by marketers by collecting and analyzing Tracked User data to determine interests, lifestyles, demographics, and other relevant categorizations to ensure relevant ads reach Tracked Users. This value can be monetized by using this information to connect marketers selling advertising relevant to a user's interests and/or demographics and to sell advertising across multiple websites to marketing firms looking to target Tracked Users based on their use of the Website or demographics.

10. In effect, the Tracking Entity receives a benefit, independent of the benefit conferred on Defendant, by using the information it obtains through tracking Tracked Users' interactions on the Website to increase the value of the advertising it sells to various other parties.

11. Similarly, the value of advertising space on Defendant's Website improves by allowing advertisers to purchase advertising space with improved effectiveness when targeting the Website's Tracked Users.

12. The use of tools like the Pixel highlights the importance of a transparent data sharing policy for a website or online store and why it is an important factor for individuals deciding whether to provide personal information to that website.

[1] Interception of Tracked Users' communications with Defendant's Website will also be used outside of the Website by the Tracking Entity to target Tracked Users with advertising sold to advertising purchasers, as discussed, *infra*, in ¶¶ 53-57.

13. Federal and state legislatures, including Missouri's and Illinois', addressed citizens' privacy expectations when communicating with other parties via wired and/or electronic communications.

14. Congress passed the federal Wiretap Act ("ECPA"), which prohibits the unauthorized interception of electronic communications.

15. The Missouri Wiretap Act, R.S. Mo. § 542.400, *et seq*, provides a civil cause of action "against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use" a "person['s]" wire communications that are "intercepted, disclosed, or used in violation of sections 542.400 to 542.422 . . . ."

16. The Illinois Eavesdropping Statute ("IES"), 720 ILCS § 5/14-1, *et seq*., prohibits the surreptitious interception, recording, or transcription of private electronic communications without the consent of all parties to that conversation and provides a civil cause of action to any person subjected to a violation of the IES against the eavesdroppers and their principals.

17. Eyemart purposefully implemented and utilized various tracking tools on its Website, including the Meta Pixel.

18. The Website does not obtain consent to expose Tracked Users' Queries to third parties as Tracked Users submit their search requests to the Website.

19. Nor does the Website obtain consent from Tracked Users when it allows Meta to monitor Tracked Users' attempts to schedule eye doctor appointments.

20. Eyemart knew that the search feature used on the Website, in conjunction with the Pixel, would allow the Tracking Entity to intercept Tracked Users' Queries, Website browsing, and Website activity in real-time, and that the Website did not provide notice of or obtain Tracked Users' consent as to such practices.

21. Thus, Tracked Users, including Plaintiffs, have been harmed by Eyemart, resulting in violations of the ECPA, the Illinois Eavesdropping Act, and the Missouri Wiretap Act. In addition to monetary damages, Plaintiffs seek injunctive relief requiring Eyemart to immediately (i) remove the tracking tools from the Website, (ii) adjust the operation of the tracking tools on the Website to prevent the sharing of legally protected information, or (iii) add appropriate and conspicuous disclosures about the nature of its Search Bar and eye exam scheduling, and obtain appropriate consent from the Tracked Users.

22. Tracked Users, including Plaintiffs, had their reasonable privacy interests violated.

23. Tracked Users, including Plaintiffs, have an interest in maintaining control over their private and sensitive information, such as their Queries and where they receive medical eye care, as well as an interest in preventing that data's misuse.

24. Plaintiffs' claims are brought as a class action, pursuant to Federal Rule of Civil Procedure 23, on behalf of themselves and all other similarly situated persons. Plaintiffs seek relief in this action individually and on behalf of Tracked Users for violations of the ECPA, the Illinois Eavesdropping Act, the Missouri Wiretap Act, breach of contract, breach of implied contract, and intrusion upon seclusion.

25. Defendant violated Tracked Users' privacy interests the moment, and each time, Plaintiffs and Tracked Users entered and submitted Queries via the Website's Search Bar, clicked on individual products within the Website, and added those products to their digital shopping cart, tried to schedule an eye exam, each of which independently resulted in PHI being intercepted by the Meta Pixel.

PARTIES

26. Plaintiff Rachelle Rand is a resident of Carl Junction, Missouri. Over the past two years, Ms. Rand visited the Website, including in November of 2023 in order to purchase prescription eyewear, as well as schedule an appointment for an eye exam.[2] During her visits to the Website, Ms. Rand was not provided an opportunity to review or consent to share her personal information, or consent to the use of the tracking tools, or to the sharing of any of her personal information such as her statutorily protected health information. Ms. Rand visited the Website to search for products and to schedule an appointment with a doctor, resulting in the disclosure of the name and location of the Eyemart location Ms. Rand used to obtain examinations and prescription eyewear from Eyemart. Ms. Rand browsed the Website's selection of prescription products, resulting in her PHI being shared with Facebook. Ms. Rand's Facebook profile included personally identifiable information, including her real name, personal photos, location, and gender. Ms. Rand did not consent to Defendant collecting her data while visiting and using the Website.

27. Plaintiff Esperanza Gottschau is a resident of Littleton, Colorado. Over the past two years, Ms. Gottschau visited Defendant's Website, including in October of 2023 to search for prescription eyewear products, Ms. Gottschau was not provided an opportunity to review or consent to share her personal information, or consent to the use of the tracking tools, or to the sharing of any of her personal information such as her statutorily protected health information. Ms. Gottschau visited Defendant's Website to search for products, resulting in Ms. Gottschau's PHI being shared with Facebook. Ms. Gottschau browsed the Website's selection of prescription products, resulting in her PHI being shared with Facebook. Ms. Gottschau's Facebook profile included personally identifiable information, including her real name, personal photos, location,

[2] Plaintiffs can provide additional, sensitive details about their doctor visits, and any services or products searched for obtained.

and gender. Ms. Gottschau did not consent to Defendant collecting her data while visiting and using the Website.

28. Plaintiff Ramon Soto is a resident of Chicago, Illinois. Over the past two years, Mr. Soto visited Defendant's Website, including in June of 2022 to search for prescription eyewear products, Mr. Soto was not provided an opportunity to review or consent to share his personal information, or consent to the use of the tracking tools, or to the sharing of any of his personal information such as his statutorily protected health information. Mr. Soto visited Defendant's Website to search for products, resulting in Mr. Soto's PHI being shared with Facebook. Mr. Soto browsed the Website's selection of prescription products, resulting in his PHI being shared with Facebook. Mr. Soto's Facebook profile included personally identifiable information, including his real name, personal photos, education history, work location and information, and city and state of residency. Mr. Soto did not consent to Defendant collecting his data while visiting and using the Website.

29. Plaintiff Georgianna Lash is a resident of South Carolina. In 2023, Ms. Lash visited Defendant's Website, to search for and purchase two pairs of prescription eyewear. As a part of the process of ordering prescription eyewear, Ms. Lash entered her prescription information into the Website. Ms. Lash was not provided an opportunity to review or consent to share her personal information, or consent to the use of the tracking tools, or to the sharing of any of her personal information such as her statutorily protected health information. Ms. Lash's visit to the Website and submission of prescription information to purchase prescription eyewear resulted in Ms. Lash's PHI being shared with Facebook. Ms. Lash browsed the Website's selection of prescription products, resulting in her PHI being shared with Facebook. Ms. Lash's Facebook profile included personally identifiable information, including her real name, personal photos, family members,

relationship status, education history, hometown, and current city and state of residency. Ms. Lash did not consent to Defendant collecting her data while visiting and using the Website.

30. Plaintiff Aaron Mees is a resident of Friendswood, Texas. In Fall 2023,s, Mr. Mees visited Defendant's Website, to search for and purchase prescription eyewear. As a part of the process of ordering prescription eyewear, Mr. Mees entered his prescription information into the Website. Mr. Mees was not provided an opportunity to review or consent to share his personal information, or consent to the use of the tracking tools, or to the sharing of any of his personal information such as his statutorily protected health information. Mr. Mees's visit to the Website and submission of prescription information to purchase prescription eyewear resulted in Mr. Mees's PHI being shared with Facebook. Mr. Mees browsed the Website's selection of prescription products, resulting in his PHI being shared with Facebook. Mr. Mees's Facebook profile included personally identifiable information, including his real name, marital status, place of employment, and current city and state of residency. Mr. Mees did not consent to Defendant collecting his data while visiting and using the Website.

31. Defendant Eyemart Express, LLC is incorporated in Delaware and headquartered in Farmers Branch, Texas. Eyemart operates a website and a chain of physical stores in the United States,[3] which perform eye examinations and sell prescription and non-prescription glasses, contact lenses, and sunglasses, backed with "skilled eye doctors to ensure there is always a

[3] Eyemart has "over 200 locations nationwide" in the following states: Alaska, Alabama, Arizona, Arkansas, Colorado, California, Florida, Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, South Carolina, South Dakota, Texas, Tennessee, Utah, Virginia, Washington, West Virginia, Wisconsin, and Wyoming. This list was based on a visual review of the list of locations listed on the website. *See Find an Eyemart Express Location Near You*, EYEMART EXPRESS, https://www.eyemartexpress.com/get-glasses (last visited October 31, 2024).

professional in your area."[4] Eyemart locations allow customers to "[r]eceive all the eye and vision care services you need in one place and enjoy more flexibility."[5]

JURISDICTION AND VENUE

32. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class Members; the aggregate amount in controversy exceeds $5,000,000.00, exclusive of interest, fees, and costs; and at least one Class Member is a citizen of a state different from Defendant.

33. This Court has personal jurisdiction over Eyemart because Eyemart is incorporated in Delaware, and is headquartered in Farmers Branch, Texas. Eyemart derives revenue in the State of Texas, including Eyemart's revenue generation from its Website, and physical Eyemart locations throughout the state of Texas. Further, the harms suffered by Plaintiffs occurred, in part, in Texas as Eyemart chose to add the tracking software on their webpages in Texas.

34. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Eyemart has places of business located in this District and Eyemart conducts substantial business operations in this District.

COMMON FACTUAL ALLEGATIONS

A. Legislative Background

1. Electronic Communications Privacy Act ("ECPA")

35. The Federal Wiretap Act (the "Wiretap Act") was enacted in 1934 "as a response to Fourth Amendment concerns surrounding the unbridled practice of wiretapping to monitor telephonic communications."[6]

[4] *Eye Exam Basics*, EYEMART EXPRESS, https://www.eyemartexpress.com/lander/eye-exam-basics (last visited October 31, 2024).

[5] *Id.*

[6] Hayden Driscoll, *Wiretapping the Internet: Analyzing the Application of the Federal Wiretap Act's Party Exception Online*, WASHINGTON AND LEE JOURNAL OF CIVIL RIGHTS AND SOCIAL JUSTICE,

36. The Wiretap Act primarily concerned the government's use of wiretaps but was amended in 1986, through the Electronic Communications Privacy Act ("ECPA"), to provide a private right of action for private intrusions as though they were government intrusions.[7]

37. Congress was concerned that technological advancements were rendering the Wiretap Act out-of-date, such as "large-scale mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing."[8]

38. As a result, the ECPA primarily focused on two types of computer services which were prominent in the 1980s: (i) electronic communications such as email between users; and (ii) remote computing services such as cloud storage or third party processing of data and files.[9]

39. Title I of the ECPA amended the Wiretap Act such that a violation occurs when a person or entity: (i) provides an electronic communication service to the public; and (ii) intentionally divulges the contents of any communication;[10] (iii) while the communication is being transmitted on that service (the "contemporaneous requirement")[11]; (iv) to any person or entity other than the intended recipient of such communication (the "party exception").[12]

40. However, the party exception does not apply to a party that intercepts or causes interception if the "communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. § 2511(2)(d).

https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=1541&context=crsj (last visited October 31, 2024).

[7] *Id.* at 192.

[8] Senate Rep. No. 99-541, at 2 (1986).

[9] *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1103 (9th Cir. 2014).

[10] 18 USCS § 2511(1).

[11] 18 USCS § 2511(3)(a).

[12] 18 USCS § 2511(2)(d).

2. Health Insurance Portability and Accountability Act ("HIPAA")

41. HIPAA, Public Law 104-191, was enacted on August 21, 1996, in part to regulate how individually identifiable health information was handled.[13] HIPAA requires the Secretary of U.S. Department of Health and Human Services ("HHS") to issue privacy regulations governing individually identifiable health information within three years of the passage of HIPAA, if Congress did not enact privacy legislation.[14] Because Congress did not enact any legislation, HHS proposed its Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule"), release it for public comment, and the Privacy Rule was finalized and published on December 28, 2000.[15]

42. HIPAA applies to "covered entities" which is defined as: (1) a health plan; (2) a health care clearinghouse; or (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA. 45 CFR §160.103.

43. HIPAA protects individually identifiable health information ("PHI"), where that information identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual, and reveals (1) past, present, or future physical or mental health or condition of an individual; (2) the provision of health care to an individual; or (3) the past, present, or future payment for the provision of health to an individual. 45 CFR §160.103.

[13] *Health Information Privacy: Summary of the HIPAA Privacy Rule*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html#:~:text=The%20Health%20Insurance%20Portability%20and%20Accountability%20Act%20of%201996%20(HIPAA,and%20security%20of%20health%20information (last visited October 31, 2024).

[14] *Id.*

[15] *Id.*

44. On December 1, 2022, the HHS Office for Civil Rights issued a bulletin "to highlight the obligations of . . . HIPAA . . . on covered entities . . . under the HIPAA Rules . . . when using online tracking technologies."[16]

45. HHS specified that "[t]hese online tracking technologies, like . . . [the] Meta Pixel, collect and analyze information about how internet users are interacting with a regulated entity's website or mobile application." [17]

46. HHS notes that information shared to tracking technology vendors, such as:

47. "an individual's . . . home or email address, or dates of appointments, as well as an individual's IP address or geographic location, . . . or any unique identifying code . . . generally [qualifies as] PHI, even if the individual does not have an existing relationship with the regulated entity and even if the [PHI], such as . . . geographic location, does not include specific treatment or billing information like dates and types of health care services. This is because when a regulated entity collects the individual's [PHI] through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care."[18]

48. This applies to "authenticated webpages, which require a user to log in before they are able to access the webpage," and even to some "unauthenticated webpages, which are webpages that do not require users to login before they are able to access the webpage."[19]

[16] *HHS Office for Civil Rights Issues Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES (Dec. 1, 2022) https://www.hhs.gov/about/news/2022/12/01/hhs-office-for-civil-rights-issues-bulletin-on-requirements-under-hipaa-for-online-tracking-technologies.html (last visited October 31, 2024).

[17] *Id.*

[18] *Health Information Privacy: Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited October 31, 2024).

[19] *Id.*

49. Notably, where "[t]racking technologies on a regulated entity's unauthenticated webpage . . . addresses specific symptoms or health conditions, such as pregnancy or miscarriage, or [unauthenticated webpage] permits individuals to search for doctors or schedule appointments[,]" the tracking technology vendors would have "access to PHI[.]"[20]

B. <u>How Websites (and the Internet) Operate</u>

50. Websites are hosted on servers, in the sense that their files are stored on and accessed from servers, but the code on individual webpages of a website "run" on a user's internet browser.

51. Websites are a collection of webpages, and each webpage is essentially a document containing text written in HyperText Markup Language (HTML) code.[21]

52. Webpages each have a unique address, and two webpages cannot be stored at the same address.[22]

53. When a user navigates to a webpage, by either entering a URL address directly or clicking a hyperlink containing the address, the browser contacts the DNS server, which translates the web address of that website into an IP address.[23]

54. An IP (Internet Protocol) address is "a unique address that identifies a device on the internet . . . ."[24] An IP address is:

> …the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and

[20] *Id.*

[21] *What is the difference between webpage, website, web server, and search engine?*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Common_questions/Web_mechanics/Pages_sites_servers_and_search_engines (last visited October 31, 2024).

[22] *Id.*

[23] *How the web works*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Getting_started_with_the_web/How_the_Web_works (last visited October 31, 2024).

[24] *What is an IP Address – Definition and Explanation*, KASPERSKY, https://usa.kaspersky.com/resource-center/definitions/what-is-an-ip-address (last visited October 31, 2024).

> websites. IP addresses provide a way of doing so and form an essential part of how the internet works.[25]

55. The user's browser then sends an HTTP Request to the server hosting that IP address via specific Request URL, requesting a copy of the webpage data for that Request URL be sent to the user, which, if approved, causes the server to send a HTTP Response that authorizes the HTTP Request and begins the process of sending the webpage's files to the user in small chunks.[26]

56. This Request URL includes a domain name and path, which identify the content being accessed on a website and where it is located.

57. The Request URL typically contains parameters. Parameters are values added to a URL to transmit data to the recipient, prefaced by a question mark to signal the use of parameters (described more fully in Section E(2)(iii)). Parameters direct a web server to provide additional context-sensitive services, as depicted below:

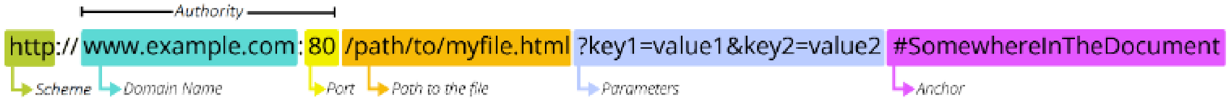


Figure 1 - Mozilla's diagram of a URL, highlighting the different elements of a URL and how they appear[27]

58. The user's browser then assembles the small chunks back into HTML, which is then processed by the user's browser and "rendered" into a visual display according to the instructions of the HTML code.[28]

C. <u>Plaintiffs Have a Privacy Right in Their Use of the Eyemart Website</u>

59. Companies can easily build profiles of customers based on their consumer habits.

[25] *Id.*
[26] *Id.*
[27] *What is a URL?*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL (last visited October 31, 2024).
[28] *Id.*

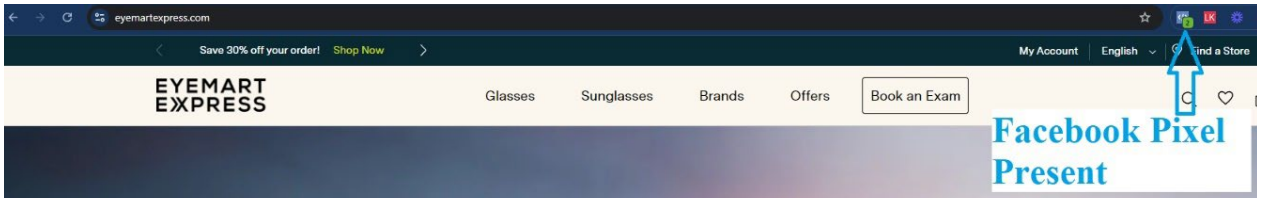
60. Communications shared between consumers and companies, by and through their websites and mobile apps, appear to be private but, in reality, the contents of those messages are regularly, without notice, shared with third parties.

61. Here, Eyemart shares Tracked Users' information, including Queries, with the Tracking Entity.

62. Queries are inherently private. This is particularly true when the searches are communicated in confidence or presumed to be private. While all Queries are personal in nature, there is an obviously heightened want for the searches to be kept confidential when the Queries themselves contain private health information.

63. Descriptions and summaries of medical products, scheduled medical appointments, and Queries relating to such are private information, indicating the health status and concerns of users, information which is federally protected, which Eyemart candidly admits.[29]

64. When first arriving at the Website, Tracked Users are free to search for the products or services they need. From this very first moment onward, the Pixel is monitoring the Tracked Users' journey through the website, as depicted below:



Facebook Pixel Present

Figure 2 – The Pixel is present on the homepage of the Website

[29] *Privacy Policy*, EYEMART EXPRESS, https://www.eyemartexpress.com/support/privacy (last visited October 31, 2024) (Noting federal law only permits disclosing PHI for "certain routine uses . . . such as those made for treatment, payment, and the operation of [its] business" without further obtaining a user's "written authorization").

65. After arriving at the Website, Tracked Users search for, look at, and purchase medical products from the Website using Queries, by viewing prescription eyewear product webpages, and adding those products to their cart.[30]

66. The Queries, when associated with descriptions of the products, pertain to more than users' basic privacy.

67. After selecting a product to purchase, a new webpage containing the product's description is loaded, allowing Tracked Users to review the specifics of glasses frames and/or select color schemes for the prescription eyewear frames.[31]

68. In addition, Tracked Users can select which types of lenses are needed for these glasses, as depicted below:

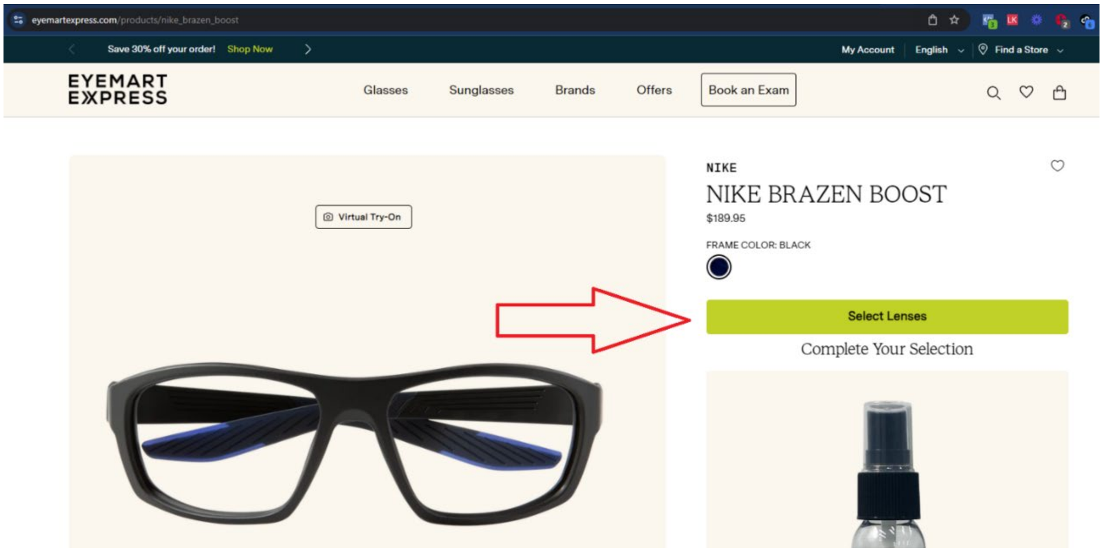
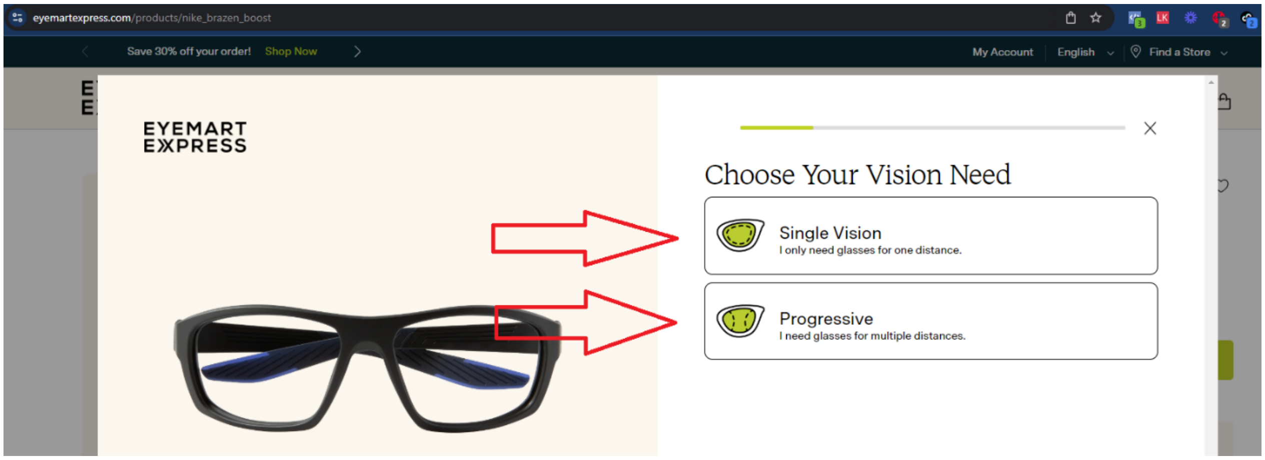


Figure 3 - Website allows Tracked Users to Select Desired Lenses on product page

69. After clicking the Select Lenses button, the Website provides the user with two options for prescription lenses, and no options for non-prescription lenses, as depicted below:

[30] *See, infra,* Figure 8.

[31] *See, infra,* Figure 8.


eyemartexpress.com/products/nike_brazen_boost
Save 30% off your order! Shop Now
My Account
English
Find a Store
EYEMART EXPRESS

Choose Your Vision Need

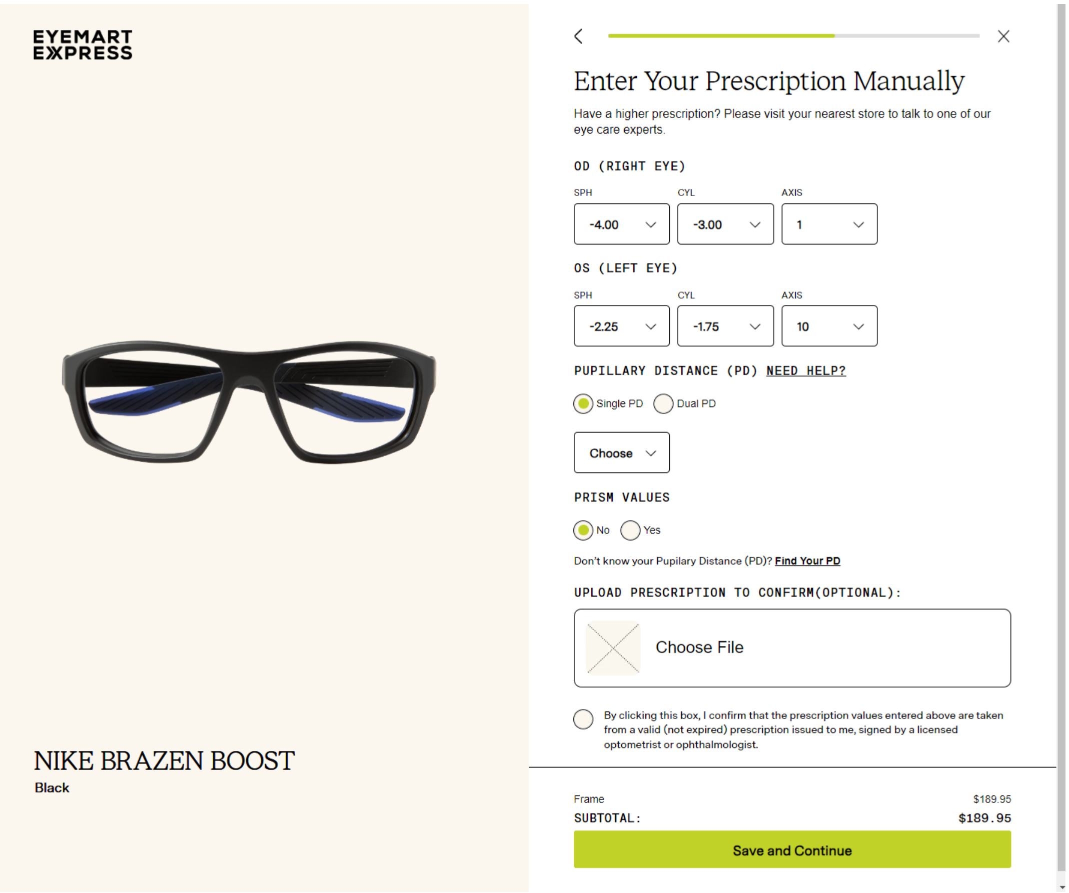
Single Vision
I only need glasses for one distance.

Progressive
I need glasses for multiple distances.

Figure 4 - Lense choice menu after clicking "Select Lenses"

70. Clicking either Single Vision or Progressive lens options advances Tracked Users to a new menu, requiring Tracked Users to provide their prescription, either through entering an online form, uploading a photo, promising to send the information later, or using an existing prescription on file.

71. Tracked Users must provide the following prescription information, including, at a minimum: 1) spherical data for left and right eyes; 2) cylinder data for left and right eyes; 3) axis data for left and right eyes; 4) pupillary distance; and 5) and prism values. Tracked Users must also confirm that any values provided to the Website were "taken from a valid (not expired) prescription issued to [the Tracked User], signed by a licensed optometrist or ophthalmologist."



EYEMART EXPRESS

NIKE BRAZEN BOOST

Black

Enter Your Prescription Manually

Have a higher prescription? Please visit your nearest store to talk to one of our eye care experts.

OD (RIGHT EYE)

SPH -4.00 CYL -3.00 AXIS 1

OS (LEFT EYE)

SPH -2.25 CYL -1.75 AXIS 10

PUPILLARY DISTANCE (PD) NEED HELP?

● Single PD ○ Dual PD

Choose

PRISM VALUES

● No ○ Yes

Don't know your Pupilary Distance (PD)? Find Your PD

UPLOAD PRESCRIPTION TO CONFIRM(OPTIONAL):

Choose File

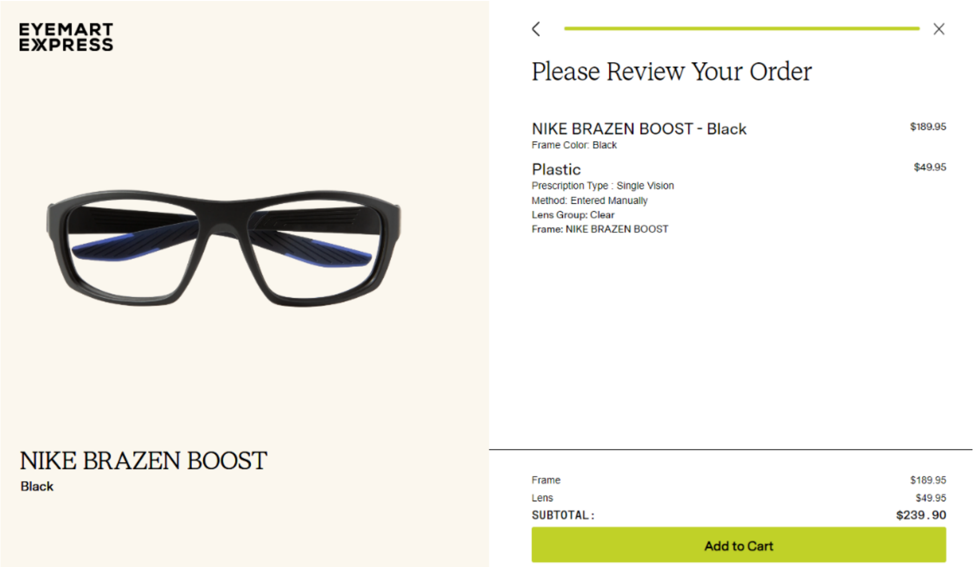
○ By clicking this box, I confirm that the prescription values entered above are taken from a valid (not expired) prescription issued to me, signed by a licensed optometrist or ophthalmologist.

Frame	$189.95
SUBTOTAL:	$189.95

Save and Continue

Figure 5 - Prescription information required to purchase glasses online through Website

72. After selecting all remaining lens options (coatings, lens material, lens color, etc.), the prescription glasses can be added to cart.



EYEMART EXPRESS

NIKE BRAZEN BOOST

Black

Please Review Your Order

NIKE BRAZEN BOOST - Black $189.95
Frame Color: Black

Plastic $49.95
Prescription Type : Single Vision
Method: Entered Manually
Lens Group: Clear
Frame: NIKE BRAZEN BOOST

Frame	$189.95
Lens	$49.95
SUBTOTAL:	$239.90

Add to Cart

Figure 6 - After entering all required information, Tracked Users can add prescription product to cart

73. After Tracked Users add their prescription products to their cart, they can have that item shipped directly to their address or any other address of their choosing.

74. Similarly, Tracked Users can navigate the Website to find a location to schedule their eye examinations, and click a link to the phone number of the location. The information associated with Tracked Users' attempts to schedule eye exams reveal their health statuses, which are highly personal, as is their choice to examine and manage health issues.

75. The descriptions and summaries of prescription products, Queries, and eye examination scheduling are then shared with the Tracking Entity and, as a result, various advertising services looking to market to Tracked Users.

D. Eyemart Is a Covered Entity and Plaintiffs' Information Constitutes PHI

76. Eyemart declares itself as a covered entity pursuant to HIPAA.[32]

77. Eyemart's HIPAA Privacy Policy notes that "[a]ny health information we collect from you on this site will be handled in accordance with the terms of our HIPAA Privacy Statement." because it is "required by applicable law to maintain the privacy of your health information."[33]

78. Notably, HIPAA prohibits the knowing and wrongful disclosure of "individually identifiable health information" to a third party. 42 U.S.C. § 1320d-6.

79. "Individually identifiable health information" is defined by HIPAA as "a subset of health information, including demographic information collected from an individual, and[] is created or received by a health care provider . . . " that "[r]elates to the past, present, or future physical or mental health or condition of an individual[or] the provision of health care to an

[32] *See Privacy Policy: HIPAA Privacy Statement*, EYEMART EXPRESS, https://www.eyemartexpress.com/support/privacy#hipaa (last visited October 31, 2024) (linking Tracked Users to Eyemart's HIPAA Privacy Policy "for information on our privacy practices, our legal duties, and your rights concerning your health information.").

[33] *Id.*

individual . . .” and that can “identify the individual” or otherwise provides “a reasonable basis to believe the information can be used to identify the individual.” 45 CFR §160.103.

80. As discussed in Section E(2), *infra*, the information disclosed by Eyemart meets the definition of individually identifiable health information.

81. While a brick-and-mortar store may more effectively separate its optometry and normal business in a physical space, the lines are blurred for online stores.

82. Notably, products one would expect to find in the optometry section of a store are found by navigating the normal portions of the Website.

E. The Tracking Entity Utilizes Tracking Tools to Benefit From Gathering Tracked Users’ Information

83. As discussed at length in Section G, the Website does not notify Tracked Users that their Queries will be surreptitiously intercepted when conducting a search on the Website. There is no conspicuous notice near the Search Bar that would let Tracked Users know that their searches were being tracked, stored, and shared.

84. The Website’s use of the Tracking Entity’s tracking tools provides benefits to the Tracking Entity that is independent of the benefit conferred to the Website.

1. Eyemart and Meta Benefit From Disclosing Plaintiffs’ PHI

85. Meta largely makes its revenue from selling advertising.[34]

86. To increase the value and effectiveness of its advertising, Meta allows its advertising customers to target “audiences” that are likely to respond to the advertising.

[34] As an example, according to its quarterly report for the period ending June 30, 2023, Meta earned a total revenue of $31,999,000,000, of which $31,498,000,000 consisted of advertising, representing 98% of total revenue. *See Meta Investor Relations: Meta Reports Second Quarter 2023 Results*, FACEBOOK (Jul. 26, 2023) https://investor.fb.com/investor-news/press-release-details/2023/Meta-Reports-Second-Quarter-2023-Results/default.aspx (last visited October 31, 2024).

87. To develop these "audiences," Meta collects information on its users regarding: what "ads they click," the webpages "they engage with," "activities [its users] engage in across Meta technologies related to things like their device usage and travel preferences," "demographics," and "the mobile device they use and the speed of their network connection."[35]

88. To assist in collecting this valuable data, Meta developed its tracking tools, such as the Pixel and Conversions API, to allow third-parties to provide Meta more information on Meta's users, to ensure that the ads Meta sells "are shown to the right people," and allow Meta and third parties to "measure the results" of advertising campaigns.[36]

89. In exchange for participating in this program, third-party websites can gain insights into their advertising efforts in an attempt to "drive more sales,"[37] either by developing better targeted advertising campaigns by analyzing customer activity on the website or by retargeting customers on other websites with advertising purchased through Meta.[38] Websites also provide clear information as to who their users are by utilizing the Pixel, increasing the value of advertising space on their own webpages.

90. Thus, both Eyemart and Meta are incentivized to collect as much information from Tracked Users as possible.

2. **Eyemart utilized Meta's Pixel to monetize Tracked Users' Queries and Webpage Interactions**

91. The Pixel is employed by website operators to gather, collect, and then share user information with Facebook.[39] Receiving this information enables Facebook and the web

[35] *Business Help Center: About detailed targeting*, FACEBOOK, https://www.facebook.com/business/help/182371508761821?id=176276233019487 (last visited October 31, 2024).
[36] *Business Help Center: About Meta Pixel*, FACEBOOK, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited October 31, 2024).
[37] *Id.*
[38] *Introduction: What is the Meta Pixel?*, FACEBOOK, https://www.facebook.com/business/tools/meta-pixel (last visited October 31, 2024).
[39] The Facebook Pixel allows websites to track Tracked User activity by monitoring user actions ("events") that websites want tracked and share a tracked user's data with Facebook. *See Meta for Developers: Meta Pixel*, FACEBOOK, https://developers.facebook.com/docs/meta-pixel/ (last visited October 31, 2024).

developers to build valuable personal profiles for users, enhancing marketing effectiveness and increasing the chance of converting users into paying customers.[40]

92. The Pixel can only be purposely added by website developers to a website. A website operator must link a related Facebook account with its Pixel, and then add code to each webpage on the website to make use of the Pixel.[41]

93. The owner or operator of a website holds the decision-making authority over the placement of the Pixel on its site, including which webpages the pixel should be added to, which events should be monitored, and what information is disclosed, including whether such information is concealed using a "hash."[42] Defendant did not hash users' information here.

i. The Website Implemented the Pixel

94. To activate and employ a Pixel, a website owner must first sign up for a Facebook account, where specific "business manager" accounts are provided the most utility for using the Pixel.[43] For instance, business manager accounts can: (i) create and utilize more simultaneous Pixels, (ii) manage multiple Facebook Ad Accounts and Pages from a centralized interface, (iii) access and manage multiple parties (which can then be given specific levels of access, including more easily revoking access to ex-employees), (iv) build custom audiences for multiple ad campaigns, and (v) eliminate privacy concerns related to using a personal profile for business purposes.[44]

[40] *See Introduction: What is the Meta Pixel*, FACEBOOK, https://www.facebook.com/business/tools/meta-pixel (last visited October 31, 2024).

[41] *How to set up and install a Meta Pixel*, FACEBOOK, https://www.facebook.com/business/help/952192354843755?id=1205376682832142 (last visited October 31, 2024).

[42] Hashing takes values of various lengths and converts them to a fixed-length value (based on number of characters), and in this process encrypts the data. *See Hash*, MOZILLA, https://developer.mozilla.org/en-US/docs/Glossary/Hash (last visited October 31, 2024).

[43] *Business Help Center: How to set up your Meta Pixel with a business portfolio*, FACEBOOK, https://www.facebook.com/business/help/314143995668266?id=1205376682832142 (last visited October 31, 2024).

[44] Jacqueline Zote, *A step-by-step guide on how to use Facebook Business Manager* (June 14, 2021), SPROUTSOCIAL https://sproutsocial.com/insights/facebook-business-manager/ (last visited October 31, 2024).

95. Website developers must also agree to Meta's Business Tools Terms before making use of the Pixel, the terms of which are described in Section G.

96. Once the Pixel is created, the website operator assigns access to the Pixel to specific people for management purposes,[45] as well as connect the Pixel to a Facebook Ad account.[46]

97. To add the Pixel to its website, the website operator can choose to add the Pixel code through the "event setup tool" via "partner integration" or by manually adding the Pixel code to the website's code.

98. Manually adding base Pixel code to the website consists of a multi-step process, which includes: (i) creating the pixel; (ii) installing base code in the header of every webpage the Pixel is active, (iii) setting automatic advanced matching behavior, (iv) adding event code using an automated tool or manually,[47] (v) domain verification, and (vi) configuring web events.[48]

99. Web developers and website operators can choose to use the Pixel to share both user activity and user identity with Facebook. Here, the Website shares both.

100. Once the Pixel is operational, it can begin collecting and sharing user activity data as instructed by the website developers.

101. A Pixel cannot be placed on a website by a third-party without being given access by the website's owner.

102. Thus, Eyemart took the affirmative steps necessary to add the Pixel to its Website.

[45] *Business Help Center: Add People to Your Meta Pixel in Your Meta Business Manager*, FACEBOOK, https://www.facebook.com/business/help/279059996069252?id=2042840805783715 (last visited October 31, 2024).

[46] *Business Help Center: Add an ad account to a Meta Pixel in Meta Business Manager*, FACEBOOK, https://www.facebook.com/business/help/622772416185967 (last visited October 31, 2024).

[47] Some users claim that automated tools for adding event code provide inconsistent results and recommend adding event code manually. *See* Ivan Mana, *How to Set Up & Install the Facebook Pixel,* YOUTUBE, https://www.youtube.com/watch?v=ynTNs5FAUm8 (last visited October 31, 2024).

[48] *Business Help Center: How to set up and install a Meta Pixel*, FACEBOOK https://www.facebook.com/business/help/952192354843755?id=1205376682832142 (last visited October 31, 2024). ; *see* Ivan Mana, *How to Set Up & Install the Facebook Pixel*, YOUTUBE, https://www.youtube.com/watch?v=ynTNs5FAUm8 (last visited October 31, 2024).

103. When a Facebook user logs onto Facebook, a "c_user" cookie – which contains a user's non-encrypted Facebook User ID number ("UID" or "FID") – is automatically created and stored on the user's device for up to a year.[49]

104. A Facebook UID can be used, by anyone, to easily identify a Facebook user.

105. Any person, even without in-depth technical expertise, can utilize the UID to identify owners of the UID via their Facebook profile. Once the Pixel's routine exchange of information is complete, the UID that becomes available can be used by any individual of ordinary skill and technical proficiency to easily identify a Facebook user, by simply appending the Facebook UID to https://www.facebook.com/ (e.g., www.facebook.com/[UID_here]). That step, readily available through any internet browser, will direct the browser to the profile page, and all the information contained in or associated with the profile page, for the user associated with the particular UID.

ii. The Pixel as a Tracking Tool

106. The Pixel tracks user-activity on web pages by monitoring events which,[50] when triggered, causes the Pixel to automatically send data directly to Facebook.[51]

107. Examples of Pixel events utilized by websites include: a user loading a webpage (i) with a Pixel installed (the "PageView event"), (iii) when pre-designated buttons are clicked (the "SubscribedButtonClick"), or (iv) when users add items to a digital cart (the "AddToCart" event), by passing along detailed query string parameters or metadata tags,[52] or (v) using custom designed Pixel events such as when users seek to find the location for an eye exam or a location to purchase

[49] *Privacy Center: Cookies Policy*, FACEBOOK, *https://www.facebook.com/privacy/policies/cookies/?subpage=subpage-1.1* (last visited October 31, 2024).
[50] *Business Help Center: About Meta Pixel*, FACEBOOK https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited October 31, 2024).
[51] *See generally Id.*
[52] *Meta for Developers: Reference - standard events*, FACEBOOK, https://developers.facebook.com/docs/meta-pixel/reference/ (last visited October 31, 2024).

their glasses (the "FindLocation" event) (with the PageView, SubscribedButtonClick, and AddToCart Events, collectively the "Pixel Events"). The Website utilizes these Pixel Events.[53]

108. When a Pixel Event is triggered, an "HTTP Request" is sent to Facebook (through Facebook's URL www.facebook.com/tr/).[54]

109. The HTTP Request includes a Request URL and embedded cookies such as the c_user cookie. It may also include information in its Payload,[55] such as metadata tags, or it may contain a "parsed" version of the Request URL.[56]

iii. The Pixel Shares Tracked Users' Website Interactions

110. When a Pixel event triggers, the parameters included in a Request URL provide websites and Facebook with additional information about the event being triggered.[57]

111. The URL's path contains information about user activity, such as which content is searched for or clicked, in addition to the parameters.

112. By way of example, the following screenshots depict how parameters are used to share Queries and how the URL path mirrors the name of the product being viewed on the Website:

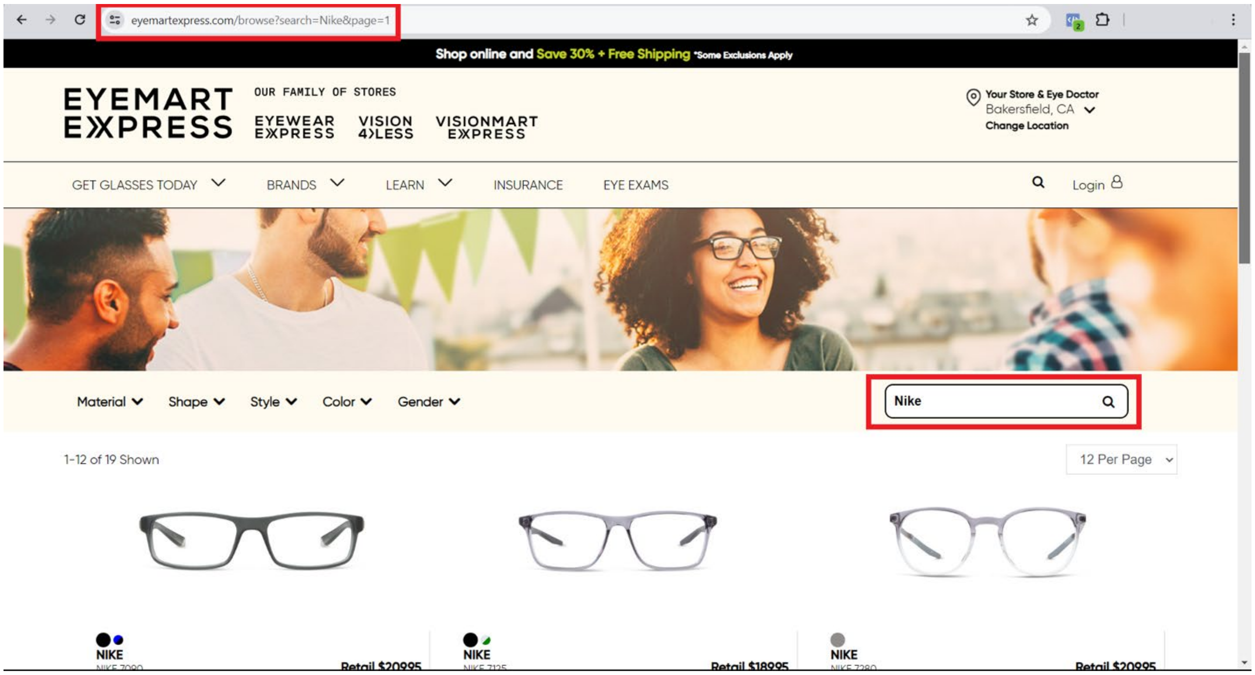
[53] The presence of Pixel events can be confirmed by using the publicly available and free Meta Pixel Helper tool. *See About the Meta Pixel Helper*, FACEBOOK, https://www.facebook.com/business/help/198406697184603?id=1205376682832142 (last visited October 31, 2024).

[54] Surya Mattu, et al., *How We Built a Meta Pixel Inspector*, THE MARKUP, https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector (last visited October 31, 2024).

[55] The "request payload" (or more simply, "Payload") is data sent by a HTTP Request, normally through a POST or PUT request, where the HTTP Request has a distinct message body. Payloads typically transmit form data, image data, and programming data. *See Request Payload Variation*, SITESPECT, *https://doc.sitespect.com/knowledge/request-payload-trigger* (last visited October 31, 2024).

[56] Data in request headers and payload headers is often unreadable and unstructured, which is why internet browsers and other software "convert data into a more readable and organized format, helping to extract relevant information while investing minimal time in interpreting a data set. *See What is data parsing?*, TIBCO, https://www.tibco.com/reference-center/what-is-data-parsing#:~:text=Data%20parsing%20is%20converting%20data,challenging%20to%20read%20and%20comprehend (last visited October 31, 2024).

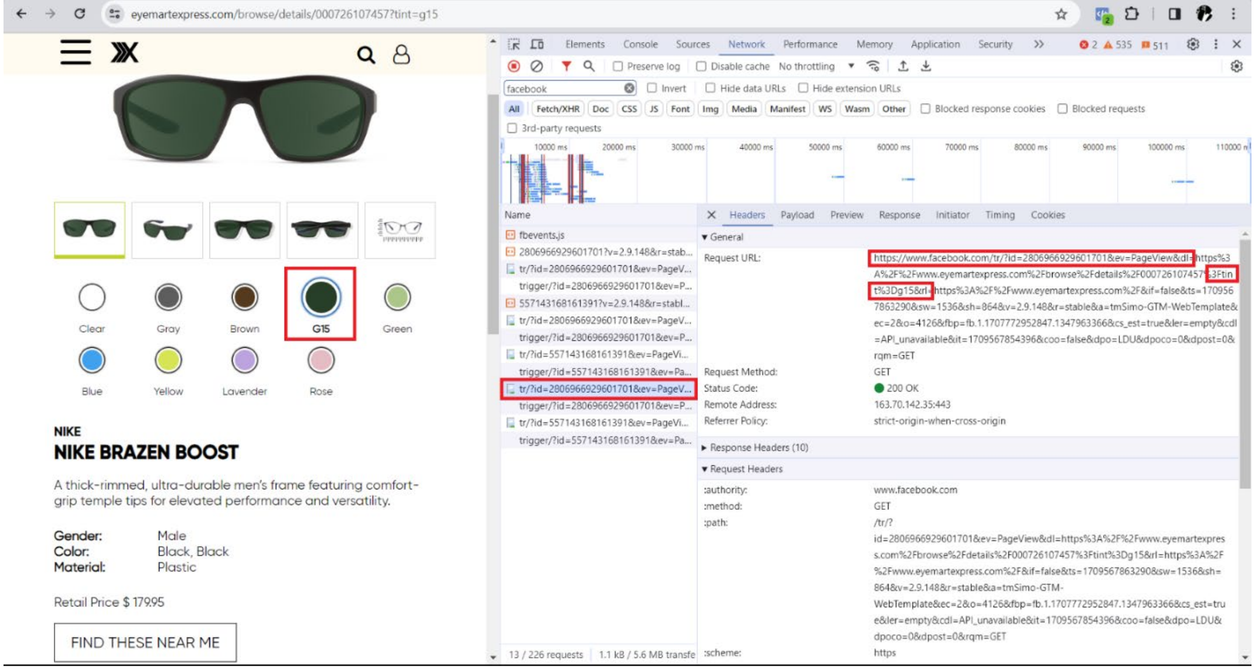
[57] *Meta for Developers: Conversion Tracking*, FACEBOOK, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking/ (last visited October 31, 2024).



eyemartexpress.com/browse?search=Nike&page=1

Nike

Figure 7 - Eyemart Website users URL parameters to convey Query information[58]



eyemartexpress.com/browse/details/000726107457?tint=g15

facebook

```
Request URL:      https://www.facebook.com/tr/?id=2806966929601701&ev=PageView&dl=https%3
                  A%2F%2Fwww.eyemartexpress.com%2Fbrowse%2Fdetails%2F000726107457%3Ftin
                  t%3Dg15&rl=https%3A%2F%2Fwww.eyemartexpress.com%2F&if=false&ts=170956
                  7863290&sw=1536&sh=864&v=2.9.148&r=stable&a=tmSimo-GTM-WebTemplate&
                  ec=2&o=4126&fbp=fb.1.1707772952847.1347963366&cs_est=true&ler=empty&cdl
                  =API_unavailable&it=1709567854396&coo=false&dpo=LDU&dpoco=0&dpost=0&
                  rqm=GET
Request Method:   GET
Status Code:      200 OK
Remote Address:   163.70.142.35:443
Referrer Policy:  strict-origin-when-cross-origin
▸ Response Headers (10)
▾ Request Headers
:authority:       www.facebook.com
:method:          GET
:path:            /tr/?
                  id=2806966929601701&ev=PageView&dl=https%3A%2F%2Fwww.eyemartexpres
                  s.com%2Fbrowse%2Fdetails%2F000726107457%3Ftint%3Dg15&rl=https%3A%2F
                  %2Fwww.eyemartexpress.com%2F&if=false&ts=1709567863290&sw=1536&sh=
                  864&v=2.9.148&r=stable&a=tmSimo-GTM-
                  WebTemplate&ec=2&o=4126&fbp=fb.1.1707772952847.1347963366&cs_est=tru
                  e&ler=empty&cdl=API_unavailable&it=1709567854396&coo=false&dpo=LDU&
                  dpoco=0&dpost=0&rqm=GET
:scheme:          https
```

NIKE

NIKE BRAZEN BOOST

A thick-rimmed, ultra-durable men's frame featuring comfort-grip temple tips for elevated performance and versatility.

Gender: Male
Color: Black, Black
Material: Plastic

Retail Price $ 179.95

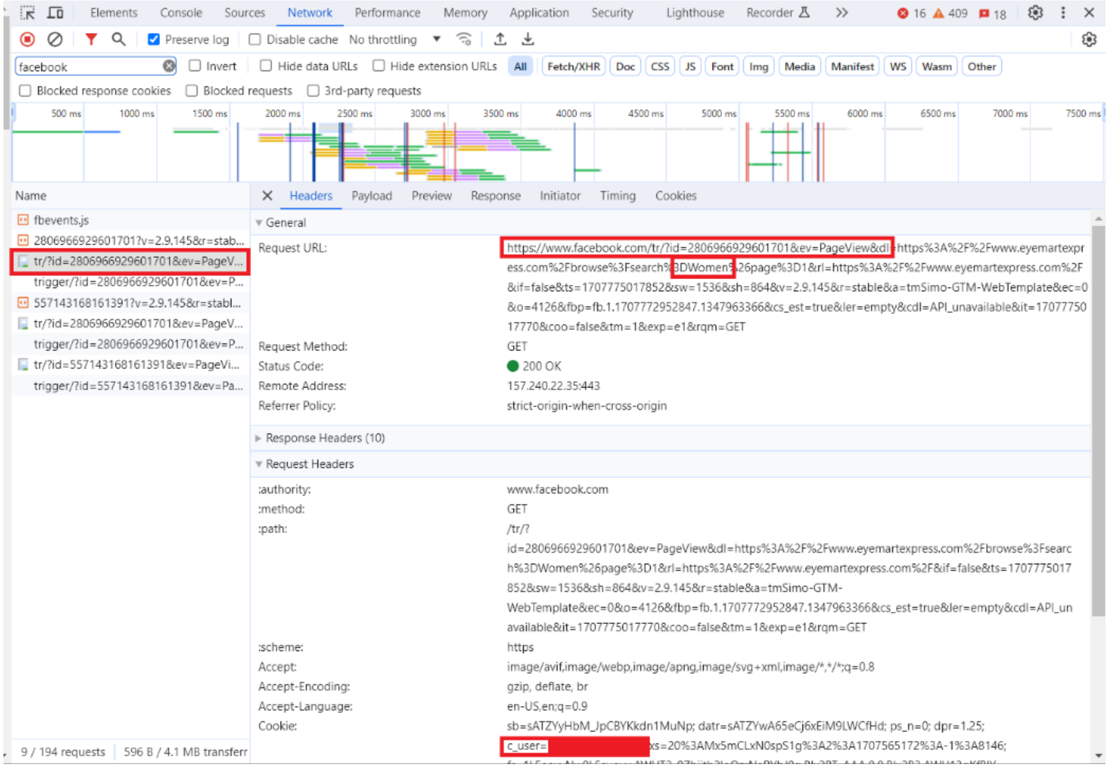
Figure 8 - Eyemart Website discloses production information through URL Path[59]

[58] *Search Results: Nike,* EYEMART EXPRESS, https://www.eyemartexpress.com/browse?search=Nike&page=1 (last visited October 31, 2024).

[59] *Search Result: Nike, Gray Tint*, EYEMART EXPRESS, *https://www.eyemartexpress.com/browse/details/000724283893?tint=gray* (last visited October 31, 2024).

113. The parameters and/or path for a Request URL may include the category or name of a product being searched for, depending on what Queries a Tracked User uses in the Search Bar.

114. The PageView, SubscribedButtonClick, AddToCart, and FindLocation events disclose Tracked Users' Request URLs. ThePageView event discloses Tracked Users' Queries as shown in *Figure 9* The FindLocation event discloses where users are looking to schedule their eye exams and when such attempts are made, as depicted below in *Figure 10*. The SubscribedButtonClick event captures when a Tracked User attempts to schedule an eye exam including the location of the Eyemart location as depicted in *Figure 11*. The AddToCart event discloses when a Tracked User adds frames and prescription lenses to their cart for purchase as depicted in *Figures 12 and 13*.



☑ Preserve log □ Disable cache □ Invert □ Hide data URLs □ Hide extension URLs □ Blocked response cookies □ Blocked requests □ 3rd-party requests

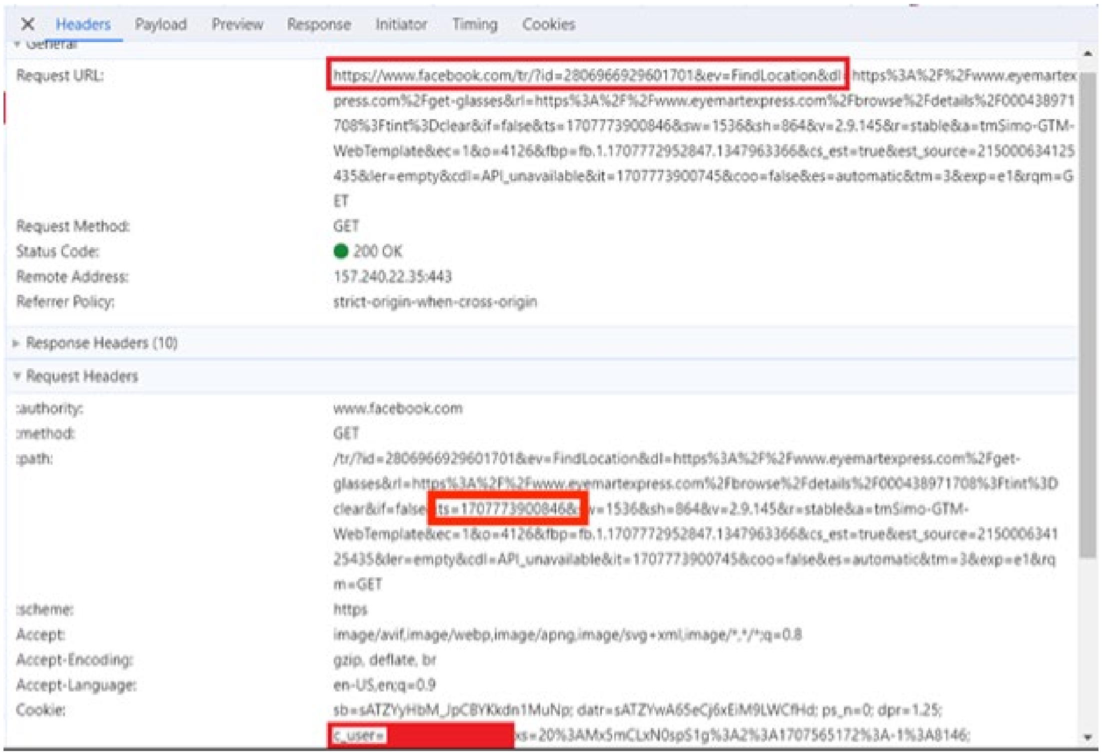
Filter: facebook

```
Name
fbevents.js
2806966929601701?v=2.9.145&r=stab...
tr/?id=2806966929601701&ev=PageV...
trigger/?id=2806966929601701&ev=P...
557143168161391?v=2.9.145&r=stabl...
tr/?id=2806966929601701&ev=PageV...
trigger/?id=2806966929601701&ev=P...
tr/?id=557143168161391&ev=PageVi...
trigger/?id=557143168161391&ev=Pa...

9 / 194 requests | 596 B / 4.1 MB transferr
```

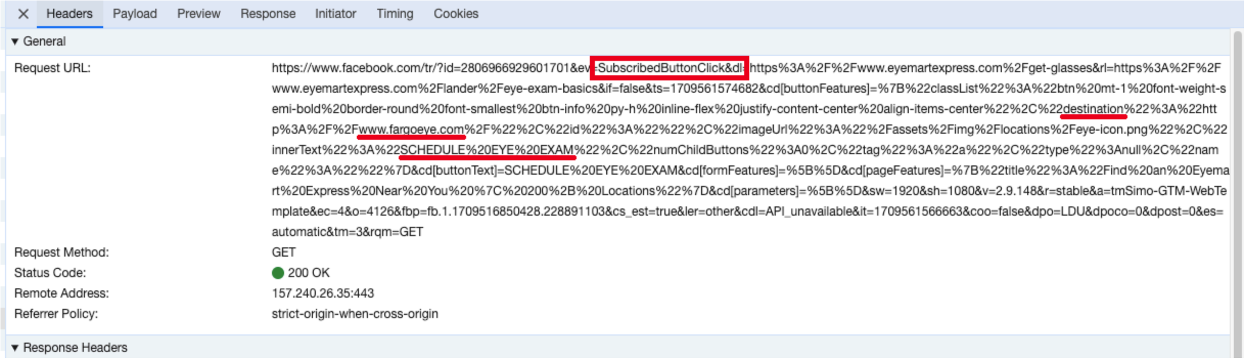
```
▼ General
Request URL:        https://www.facebook.com/tr/?id=2806966929601701&ev=PageView&dl=https%3A%2F%2Fwww.eyemartexpr
                    ess.com%2Fbrowse%3Fsearch%3DWomen%26page%3D1&rl=https%3A%2F%2Fwww.eyemartexpress.com%2F
                    &if=false&ts=1707775017852&sw=1536&sh=864&v=2.9.145&r=stable&a=tmSimo-GTM-WebTemplate&ec=0
                    &o=4126&fbp=fb.1.1707772952847.1347963366&cs_est=true&ler=empty&cdl=API_unavailable&it=17077750
                    17770&coo=false&tm=1&exp=e1&rqm=GET
Request Method:     GET
Status Code:        ● 200 OK
Remote Address:     157.240.22.35:443
Referrer Policy:    strict-origin-when-cross-origin
▶ Response Headers (10)
▼ Request Headers
:authority:         www.facebook.com
:method:            GET
:path:              /tr/?
                    id=2806966929601701&ev=PageView&dl=https%3A%2F%2Fwww.eyemartexpress.com%2Fbrowse%3Fsearc
                    h%3DWomen%26page%3D1&rl=https%3A%2F%2Fwww.eyemartexpress.com%2F&if=false&ts=1707775017
                    852&sw=1536&sh=864&v=2.9.145&r=stable&a=tmSimo-GTM-
                    WebTemplate&ec=0&o=4126&fbp=fb.1.1707772952847.1347963366&cs_est=true&ler=empty&cdl=API_un
                    available&it=1707775017770&coo=false&tm=1&exp=e1&rqm=GET
:scheme:            https
Accept:             image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding:    gzip, deflate, br
Accept-Language:    en-US,en;q=0.9
Cookie:             sb=sATZYyHbM_JpCBYKkdn1MuNp; datr=sATZYwA65eCj6xEiM9LWCfHd; ps_n=0; dpr=1.25;
                    c_user=[redacted]xs=20%3AMx5mCLxN0spS1g%3A2%3A1707565172%3A-1%3A8146;
```

Figure 9 - PageView event triggered on the Website, disclosing Query to Facebook



```
▾ General
Request URL:        https://www.facebook.com/tr/?id=2806966929601701&ev=FindLocation&dl=https%3A%2F%2Fwww.eyemartex
                    press.com%2Fget-glasses&rl=https%3A%2F%2Fwww.eyemartexpress.com%2Fbrowse%2Fdetails%2F000438971
                    708%3Ftint%3Dclear&if=false&ts=1707773900846&sw=1536&sh=864&v=2.9.145&r=stable&a=tmSimo-GTM-
                    WebTemplate&ec=1&o=4126&fbp=fb.1.1707772952847.1347963366&cs_est=true&est_source=215000634125
                    435&ler=empty&cdl=API_unavailable&it=1707773900745&coo=false&es=automatic&tm=3&exp=e1&rqm=G
                    ET
Request Method:     GET
Status Code:        ● 200 OK
Remote Address:     157.240.22.35:443
Referrer Policy:    strict-origin-when-cross-origin
▸ Response Headers (10)
▾ Request Headers
:authority:         www.facebook.com
:method:            GET
:path:              /tr/?id=2806966929601701&ev=FindLocation&dl=https%3A%2F%2Fwww.eyemartexpress.com%2Fget-
                    glasses&rl=https%3A%2F%2Fwww.eyemartexpress.com%2Fbrowse%2Fdetails%2F000438971708%3Ftint%3D
                    clear&if=false&ts=1707773900846&sw=1536&sh=864&v=2.9.145&r=stable&a=tmSimo-GTM-
                    WebTemplate&ec=1&o=4126&fbp=fb.1.1707772952847.1347963366&cs_est=true&est_source=2150006341
                    25435&ler=empty&cdl=API_unavailable&it=1707773900745&coo=false&es=automatic&tm=3&exp=e1&rq
                    m=GET
:scheme:            https
Accept:             image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding:    gzip, deflate, br
Accept-Language:    en-US,en;q=0.9
Cookie:             sb=sATZYyHbM_JpCBYKkdn1MuNp; datr=sATZYwA65eCj6xEiM9LWCfHd; ps_n=0; dpr=1.25;
                    c_user=[redacted]xs=20%3AMx5mCLxN0spS1g%3A2%3A1707565172%3A-1%3A8146;
```

Figure 10 - FindLocation event tracks when Tracked Users attempts to schedule eye exams or purchase prescription eyewear in a physical store



```
▾ General
Request URL:        https://www.facebook.com/tr/?id=2806966929601701&ev=SubscribedButtonClick&dl=https%3A%2F%2Fwww.eyemartexpress.com%2Fget-glasses&rl=https%3A%2F%2F
                    www.eyemartexpress.com%2Flander%2Feye-exam-basics&if=false&ts=1709561574682&cd[buttonFeatures]=%7B%22classList%22%3A%22btn%20mt-1%20font-weight-s
                    emi-bold%20border-round%20font-smallest%20btn-info%20py-h%20inline-flex%20justify-content-center%20align-items-center%22%2C%22destination%22%3A%22htt
                    p%3A%2F%2Fwww.fargoeye.com%2F%22%2C%22id%22%3A%22%22%2C%22imageUrl%22%3A%22%2Fassets%2Fimg%2Flocations%2Feye-icon.png%22%2C%22
                    innerText%22%3A%22SCHEDULE%20EYE%20EXAM%22%2C%22numChildButtons%22%3A0%2C%22tag%22%3A%22a%22%2C%22type%22%3Anull%2C%22nam
                    e%22%3A%22%22%7D&cd[buttonText]=SCHEDULE%20EYE%20EXAM&cd[formFeatures]=%5B%5D&cd[pageFeatures]=%7B%22title%22%3A%22Find%20an%20Eyema
                    rt%20Express%20Near%20You%20%7C%20200%2B%20Locations%22%7D&cd[parameters]=%5B%5D&sw=1920&sh=1080&v=2.9.148&r=stable&a=tmSimo-GTM-WebTe
                    mplate&ec=4&o=4126&fbp=fb.1.1709516850428.228891103&cs_est=true&ler=other&cdl=API_unavailable&it=1709561566663&coo=false&dpo=LDU&dpoco=0&dpost=0&es=
                    automatic&tm=3&rqm=GET
Request Method:     GET
Status Code:        ● 200 OK
Remote Address:     157.240.26.35:443
Referrer Policy:    strict-origin-when-cross-origin
▾ Response Headers
```

Figure 11 - SubscribedButtonClick tracks when Tracked Users attempt to schedule eye exam with specific Eyemart locations

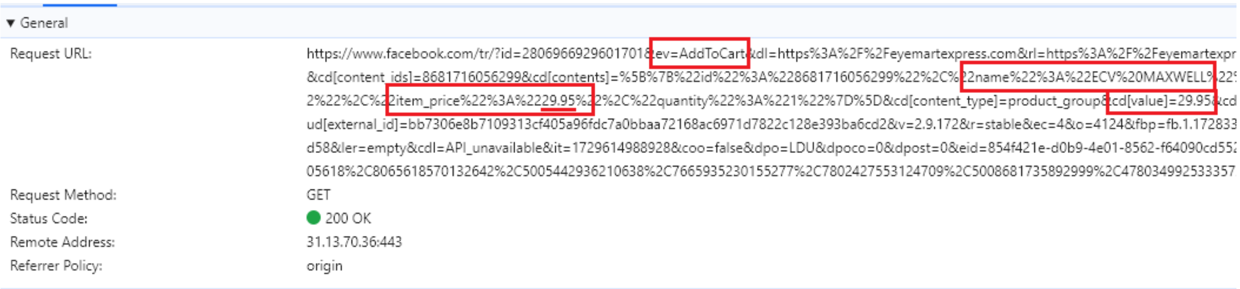
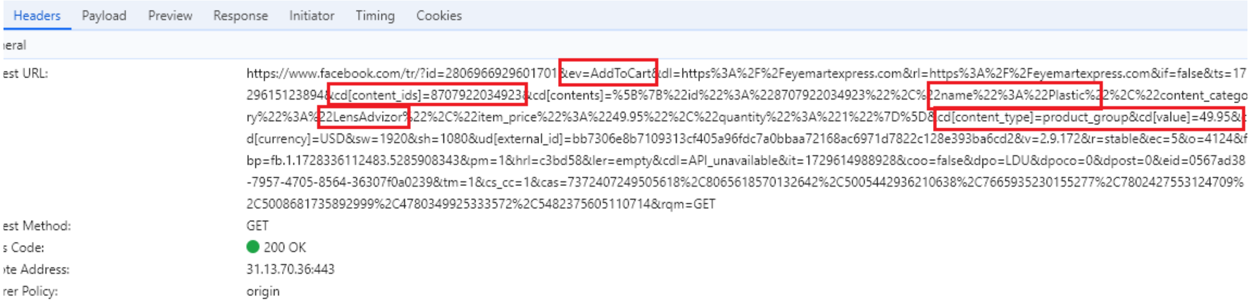

```
▾ General
Request URL:        https://www.facebook.com/tr/?id=2806966929601701&ev=AddToCart&dl=https%3A%2F%2Feyemartexpress.com&rl=https%3A%2F%2Feyemartexpr
                    &cd[content_ids]=8681716056299&cd[contents]=%5B%7B%22id%22%3A%228681716056299%22%2C%22name%22%3A%22ECV%20MAXWELL%22%
                    2%22%2C%22item_price%22%3A%2229.95%22%2C%22quantity%22%3A%221%22%7D%5D&cd[content_type]=product_group&cd[value]=29.95&cd
                    ud[external_id]=bb7306e8b7109313cf405a96fdc7a0bbaa72168ac6971d7822c128e393ba6cd2&v=2.9.172&r=stable&ec=4&o=4124&fbp=fb.1.172833
                    d58&ler=empty&cdl=API_unavailable&it=1729614988928&coo=false&dpo=LDU&dpoco=0&dpost=0&eid=854f421e-d0b9-4e01-8562-f64090cd55
                    05618%2C8065618570132642%2C5005442936210638%2C7665935230155277%2C7802427553124709%2C5008681735892999%2C478034992533357
Request Method:     GET
Status Code:        ● 200 OK
Remote Address:     31.13.70.36:443
Referrer Policy:    origin
```

Figure 12 - AddToCart event discloses when Tracked Users add frames to digital cart



```
est URL:        https://www.facebook.com/tr/?id=2806966929601701&ev=AddToCart&dl=https%3A%2F%2Feyemartexpress.com&rl=https%3A%2F%2Feyemartexpress.com&if=false&ts=17
                29615123894&cd[content_ids]=8707922034923&cd[contents]=%5B%7B%22id%22%3A%228707922034923%22%2C%22name%22%3A%22Plastic%22%2C%22content_catego
                ry%22%3A%22LensAdvizor%22%2C%22item_price%22%3A%2249.95%22%2C%22quantity%22%3A%221%22%7D%5D&cd[content_type]=product_group&cd[value]=49.95&
                d[currency]=USD&sw=1920&sh=1080&ud[external_id]=bb7306e8b7109313cf405a96fdc7a0bbaa72168ac6971d7822c128e393ba6cd2&v=2.9.172&r=stable&ec=5&o=4124&f
                bp=fb.1.1728336112483.5285908343&pm=1&hrl=c3bd58&ler=empty&cdl=API_unavailable&it=1729614988928&coo=false&dpo=LDU&dpoco=0&dpost=0&eid=0567ad38
                -7957-4705-8564-36307f0a0239&tm=1&cs_cc=1&cas=7372407249505618%2C8065618570132642%2C5005442936210638%2C7665935230155277%2C7802427553124709%
                2C5008681735892999%2C4780349925333572%2C5482375605110714&rqm=GET
est Method:     GET
s Code:         ● 200 OK
ote Address:    31.13.70.36:443
rer Policy:     origin
```

Figure 13 - AddToCart event discloses when Tracked Users add prescription lenses to digital cart

115. PageView events are triggered by default whenever the Pixel is loaded onto a user's web browser.[60]

116. When a PageView event is triggered, it sends a request to Facebook containing data, including, but not limited to, its properties, as depicted above in *Figure 9*.

117. FindLocation events are custom events used by Eyemart which appear to trigger whenever users load the webpage to pick a location to schedule an eye exam.[61]

118. When a FindLocation event is triggered, it sends a request to Facebook containing data, including, but not limited to, its metadata properties, as depicted above in *Figure 10*.

119. While little documentation is available for the SubscribedButtonClick events, they appear to be triggered when users click buttons to submit forms, button clicks in general, and even just clicks on various elements of webpages, including links.[62]

120. When a SubscribedButtonClick event is triggered, it sends a request to Facebook containing data, including, but not limited to, its properties, as depicted above in *Figure 11*.

[60] *Meta for Developers: Conversion Tracking*, FACEBOOK, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking/ (last visited October 31, 2024).
[61] Surya Mattu, et al., *How We Built a Meta Pixel Inspector*, THE MARKUP, https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector (last visited October 31, 2024).
[62] *Id.*

121. Similar to the SubscribedButtonClick event, the AddToCart event triggers when a user "click[s] an add to cart button on a website."[63]

122. The AddToCart event sends a request to Facebook including the product ID of the item, the price, the make and model, and details of the prescription eyewear added to the cart, as depicted in *Figures 12 and 13*.

123. When a "c_user" cookie is present on a user's computer, the HTTP Requests generated by the Pixel Events include users' c_user cookies by copying the c_user cookie into the Request Header, as depicted in *Figure 17.*

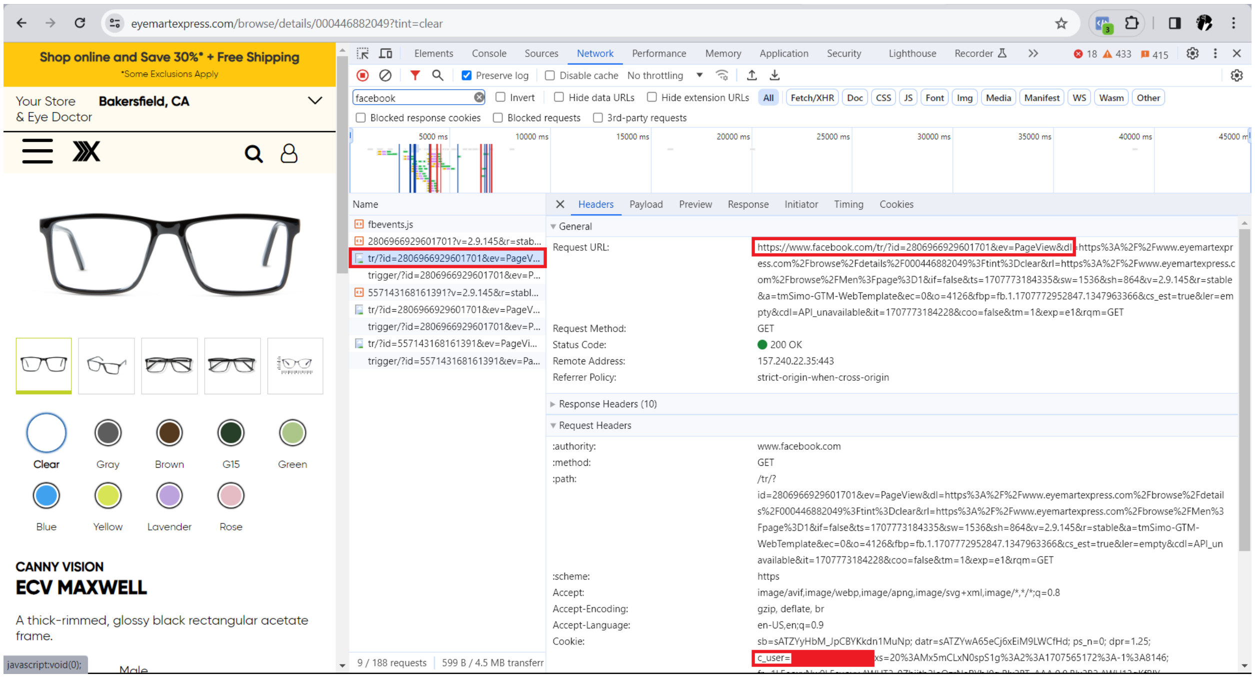
124. This "c_user" cookie contains an unencrypted, numeric unique identifier (the Facebook FID) which may be used to identify a user, as described in Section F.

125. The Pixel Events, when triggered, automatically cause a user's computer to duplicate users' FIDs, Search Terms, and/or PHI at the time that information is submitted to Eyemart, insert that information into the HTTP Request it generates, and then send that HTTP Request to "www.facebook.com/tr" as shown above in *Figure 14-16.* In short, triggering the Pixel Events results in the sharing of a user's website interactions (including PHI) and Facebook UID with Facebook.

126. This behavior is not limited to Tracked Users seeking to schedule eye exams on the Website.

127. The Pixel Events are active on other parts of the Website, including webpages where Tracked Users shop, as depicted below in Figures 14-16:

[63] Met Business Help Cnterhttps://www.facebook.com/business/help/402791146561655?id=1205376682832142 *Meta Business Help Center: Specifications for Meta Pixel standard events*, FACEBOOK, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited October 31, 2024).



eyemartexpress.com/browse/details/000446882049?tint=clear

Shop online and Save 30%* + Free Shipping
*Some Exclusions Apply

Your Store & Eye Doctor **Bakersfield, CA**

Clear Gray Brown G15 Green
Blue Yellow Lavender Rose

CANNY VISION
ECV MAXWELL

A thick-rimmed, glossy black rectangular acetate frame.

javascript:void(0);

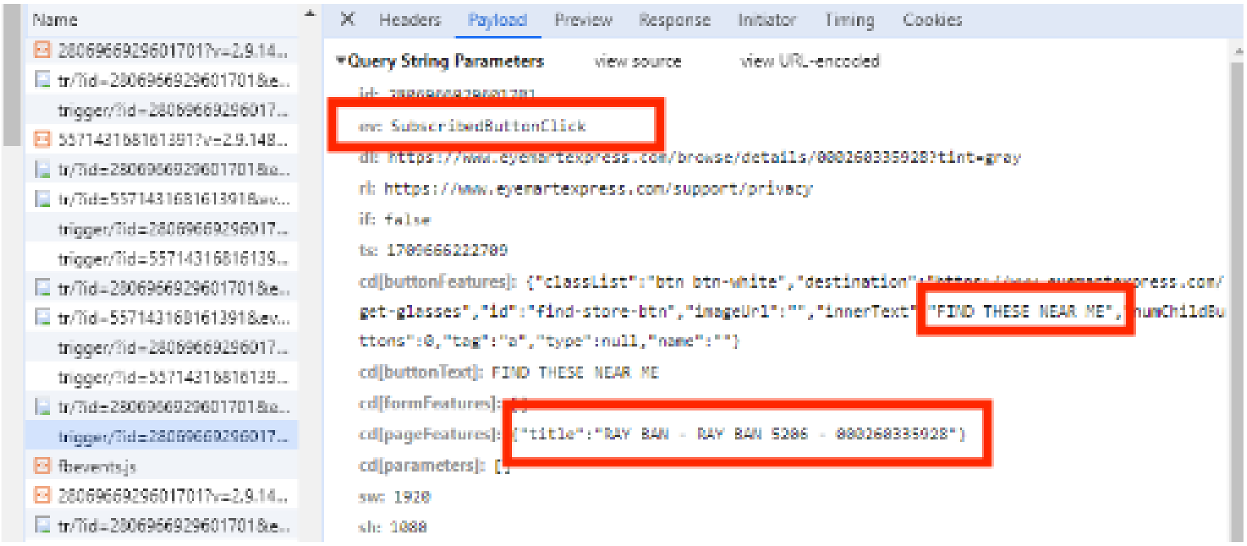
Male

```
Name
fbevents.js
2806966929601701?v=2.9.145&r=stab...
tr/?id=2806966929601701&ev=PageV...
trigger/?id=2806966929601701&ev=P...
557143168161391?v=2.9.145&r=stabl...
tr/?id=2806966929601701&ev=PageV...
trigger/?id=2806966929601701&ev=P...
tr/?id=557143168161391&ev=PageVi...
trigger/?id=557143168161391&ev=Pa...

9 / 188 requests | 599 B / 4.5 MB transferr
```

```
▼ General
Request URL:        https://www.facebook.com/tr/?id=2806966929601701&ev=PageView&dl=https%3A%2F%2Fwww.eyemartexpr
                    ess.com%2Fbrowse%2Fdetails%2F000446882049%3Ftint%3Dclear&rl=https%3A%2F%2Fwww.eyemartexpress.c
                    om%2Fbrowse%2FMen%3Fpage%3D1&if=false&ts=1707773184335&sw=1536&sh=864&v=2.9.145&r=stable
                    &a=tmSimo-GTM-WebTemplate&ec=0&o=4126&fbp=fb.1.1707772952847.1347963366&cs_est=true&ler=em
                    pty&cdl=API_unavailable&it=1707773184228&coo=false&tm=1&exp=e1&rqm=GET
Request Method:     GET
Status Code:        ● 200 OK
Remote Address:     157.240.22.35:443
Referrer Policy:    strict-origin-when-cross-origin
▶ Response Headers (10)
▼ Request Headers
:authority:         www.facebook.com
:method:            GET
:path:              /tr/?
                    id=2806966929601701&ev=PageView&dl=https%3A%2F%2Fwww.eyemartexpress.com%2Fbrowse%2Fdetail
                    s%2F000446882049%3Ftint%3Dclear&rl=https%3A%2F%2Fwww.eyemartexpress.com%2Fbrowse%2FMen%3
                    Fpage%3D1&if=false&ts=1707773184335&sw=1536&sh=864&v=2.9.145&r=stable&a=tmSimo-GTM-
                    WebTemplate&ec=0&o=4126&fbp=fb.1.1707772952847.1347963366&cs_est=true&ler=empty&cdl=API_un
                    available&it=1707773184228&coo=false&tm=1&exp=e1&rqm=GET
:scheme:            https
Accept:             image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding:    gzip, deflate, br
Accept-Language:    en-US,en;q=0.9
Cookie:             sb=sATZYyHbM_JpCBYKkdn1MuNp; datr=sATZYwA65eCj6xEiM9LWCfHd; ps_n=0; dpr=1.25;
                    c_user=[redacted]xs=20%3AMx5mCLxN0spS1g%3A2%3A1707565172%3A-1%3A8146;
```

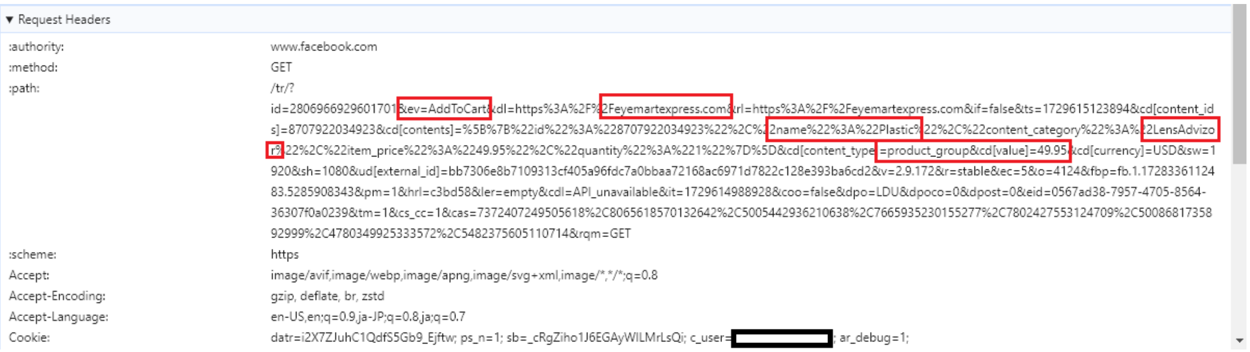
Figure 14 – PageView triggers when Tracked Users select frames



```
Name
2806966929601701?v=2.9.14...
tr/?id=2806966929601701&e...
trigger/?id=2806966929601701...
557143168161391?v=2.9.148...
tr/?id=2806966929601701&e...
tr/?id=557143168161391&ev...
trigger/?id=2806966929601701...
trigger/?id=557143168161391...
tr/?id=2806966929601701&e...
tr/?id=557143168161391&ev...
trigger/?id=2806966929601701...
trigger/?id=557143168161391...
tr/?id=2806966929601701&e...
trigger/?id=2806966929601701...
fbevents.js
2806966929601701?v=2.9.14...
tr/?id=2806966929601701&e...
```

```
▼Query String Parameters     view source     view URL-encoded
  id: 2806966929601701
  ev: SubscribedButtonClick
  dl: https://www.eyemartexpress.com/browse/details/000268335928?tint=gray
  rl: https://www.eyemartexpress.com/support/privacy
  if: false
  ts: 1709666222709
  cd[buttonFeatures]: {"classList":"btn btn-white","destination":"https://www.eyemartexpress.com/
  get-glasses","id":"find-store-btn","imageUrl":"","innerText":"FIND THESE NEAR ME","numChildBu
  ttons":0,"tag":"a","type":null,"name":""}
  cd[buttonText]: FIND THESE NEAR ME
  cd[formFeatures]: []
  cd[pageFeatures]: {"title":"RAY BAN - RAY BAN 5286 - 000268335928"}
  cd[parameters]: []
  sw: 1920
  sh: 1080
```

Figure 15 – SubscribedButtonClick event triggers when Tracked Users attempt to purchase their selected frames on the Website or search for location to buy the frames searched for



```
▼ Request Headers
:authority:          www.facebook.com
:method:             GET
:path:               /tr/?
                     id=2806966929601701&ev=AddToCart&dl=https%3A%2F%2Feyemartexpress.com&rl=https%3A%2F%2Feyemartexpress.com&if=false&ts=1729615123894&cd[content_id
                     s]=8707922034923&cd[contents]=%5B%7B%22id%22%3A%228707922034923%22%2C%22name%22%3A%22Plastic%22%2C%22content_category%22%3A%22LensAdvizo
                     r%22%2C%22item_price%22%3A%2249.95%22%2C%22quantity%22%3A%221%22%7D%5D&cd[content_type]=product_group&cd[value]=49.95&cd[currency]=USD&sw=1
                     920&sh=1080&ud[external_id]=bb7306e8b7109313cf405a96fdc7a0bbaa72168ac6971d7822c128e393ba6cd2&v=2.9.172&r=stable&ec=5&o=4124&fbp=fb.1.17283361124
                     83.5285908343&pm=1&hrl=c3bd58&ler=empty&cdl=API_unavailable&it=1729614988928&coo=false&dpo=LDU&dpoco=0&dpost=0&eid=0567ad38-7957-4705-8564-
                     36307f0a0239&tm=1&cs_cc=1&cas=7372407249505618%2C8065618570132642%2C5005442936210638%2C7665935230155277%2C7802427553124709%2C50086817358
                     92999%2C4780349925333572%2C5482375605110714&rqm=GET
:scheme:             https
Accept:              image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding:     gzip, deflate, br, zstd
Accept-Language:     en-US,en;q=0.9,ja-JP;q=0.8,ja;q=0.7
Cookie:              datr=i2X7ZJuhC1QdfS5Gb9_Ejftw; ps_n=1; sb=_cRgZiho1J6EGAyWILMrLsQi; c_user=[redacted]; ar_debug=1;
```

Figure 16 – AddToCart event trigger Tracked Users add prescription products to cart to purchase on the Website, and includes the Tracked Users' FID

128. As shown above, triggering of the PageView and AddToCart causes a specific description of the frames and lenses being sought by the Tracked User to be disclosed along with their FID.

129. As described in paragraph 112, the HTTP Requests generated by the Pixel Events depicted in Figures 14-16 include not only the user activity information but also their FID.

130. Thus, PHI of Plaintiffs and the Class Members have automatically been shared with Facebook as a result of Eyemart's decision to add the Pixel to the Website.

131. As described above, the Pixel captures information on the Website and sends that information to Meta through triggered Pixel Events.

132. The Pixel passed this information through the HTTP Requests sent to facebook.com/tr.

133. The Pixel intercepted and shared PHI related to medical products sought and viewed by Plaintiffs.

134. The Pixel is active across the Website, including prescription product pages and the relevant information associated with Tracked Users' attempts to schedule eye examinations on the website, as implemented by Eyemart.

135. When a Tracked User views or interacts with those medical products or services on the Website, those actions are intercepted and monetized by the Tracking Entity.

iv. The Pixel Transmissions Are Sent From Users' Computers

136. The site of the harm is the location of the device used by Tracked Users. This is supported by how the Pixel operates.

137. Once the Pixel was programmed onto the Website, it then surreptitiously loaded on to users' computers whenever they visit the Website.

138. The Pixel, without users' knowledge, runs or executes on users' devices, causing users' devices to duplicate the information obtained from Tracked Users' activity on a webpage nearly instantly, which is then sent by users' devices, based on instructions from the Pixel, to Meta.

139. In essence, (i) the Pixel is loaded onto a user's device, (ii) causes the user's device to violate a user's privacy by tracking their activity, and (iii) utilizes the user's device to disclose that information to a third party.

140. The location of the device executing the Pixel when used by a Tracked User to visit the Website is thereby the location of the harm.

F. <u>The FID can be easily used to Identify Users</u>

141. A person of ordinary skill, in possession of the PHI in question, is capable of converting the data into personally identifiable information without the addition of information from outside sources.

142. A person of ordinary skill need not have the technical proficiency to gain access to the data itself, only the ability to use the information once in possession to identify the user.

143. When sending HTTP Requests, the internet browser breaks the Requests into manageable pieces by encoding the Request in small packets (a process called "transfer encoding").[64]

[64] *See Transfer-Encoding,* MOZILLA, https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Transfer-Encoding (last visited October 31, 2024).

144. The images of Pixel transmissions captured by Plaintiffs in the developer's console, (*see e.g., supra*, *Figures 14 - 16*) capture the data in this encoded condition.

145. However, the information does not stay encoded and is not handled by third-party recipients of the PHI (here, Facebook) in this encoded state.

146. To start, once the transmission is received, the transfer encoding is removed by the recipient automatically, simplifying the data to an easier-to-digest fashion.

147. After the transfer encoding is automatically removed, which occurs whenever a computer processes a HTTP Request, Facebook's systems then automatically synthesize the data into simple-to-read and simple-to-use formats.[65]

148. On information and belief, the data contained within the Pixel transmissions sent to Facebook by Defendant, including the PHI and UID, is automatically processed by Facebook's algorithms before any person interacts with the data.[66]

149. Facebook logs the time and date of each Pixel event activation, the URL associated with each event, the Domains associated with each event, and the devices associated with each event – all of which are neatly compiled and categorized for website developers to access and view through the use of the Pixel.[67]

150. Facebook also makes the data provided to it through the Defendant's Pixel Events available and similarly easy to use for Facebook's advertising customers.

[65] *Human Data Banks and Algorithmic Labour: Facebook Algorithmic Factory (2)*, SHARE LAB (Aug. 20, 2016) https://labs.rs/en/facebook-algorithmic-factory-human-data-banks-and-algorithmic-labour/ (last visited October 31, 2024).

[66] *See Id.*; also *Facebook Algorithmic Factory*, SHARE LAB, https://labs.rs/wp-content/uploads/2016/08/FacebookFactory-01.gif (last visited October 31, 2024) (visual of automation process and the detail that Facebook gathers on users).

[67] *See Facebook Events Manager: How To Use The Data From Your Tracking Pixel (Data Driven Daily Tip 195*, YOUTUBE (at 3:11/6:00) https://www.youtube.com/watch?v=R1qAmVAOzO8 (last visited October 31, 2024).

151. Facebook offers website developers a tracking option which enables developers to target website users by matching those users to Facebook account holders via the Pixel.[68] This provides quick and unfettered access to users' Facebook account information. This is all facilitated through the availability and use of the UID.

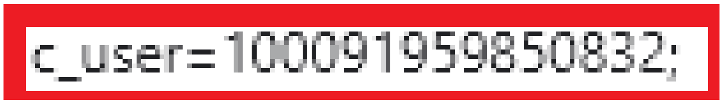
152. Facebook sells advertising to third parties who aim to target specific "audiences" based on a number of traits or factors, including demographic, interest-based, geographic, age-based, and gender-based categories, using targeted advertising data collected by website developers implementing the Pixel on their websites.[69] These traits are derived from, at least in part, Facebook profiles.

153. Facebook creates targetable audiences by combining the data captured by the Pixel (including associating website activity to accounts through the UID), and other tracking software provided by Facebook, to categorize its users into marketable segments.[70]

154. Thus, UIDs are easily accessed by Facebook and, in fact, used by Facebook.

155. A person of ordinary skill, once in possession of the UID, could easily turn the UID into personally identifiable information.

156. The UID contains a series of numbers used to identify a specific profile, as depicted below:



```
c_user=100091959850832;
```

Figure 17- Sample c_user ID number of test account created by Plaintiffs' counsel to investigate the Pixel, captured by a Pixel Event

[68] *Business Help Center: About website custom audiences*, FACEBOOK, https://www.facebook.com/business/help/610516375684216?id=2469097953376494 (last visited October 31, 2024).

[69] *See Meta Ads: The ad auction explained*, FACEBOOK, https://www.facebook.com/business/ads/ad-auction (last visited October 31, 2024).

[70] *See generally Business Help Center: About event match quality*, FACEBOOK, https://www.facebook.com/business/help/765081237991954?id=818859032317965 (last visited October 31, 2024) (noting a key metric is how well customer event information matches to a Meta account).

157. A Facebook UID can be used by anyone to easily identify a Facebook user by simply appending the Facebook UID to https://www.facebook.com/ (e.g., www.facebook.com/[UID_here]).

158. Using the UID from Figure 18, appending it to the Facebook URL in a standard internet browser (here, www.facebook.com/100091959850832) will redirect the webpage straight to the Facebook profile associated with the UID, as depicted in Figure 18, next page:

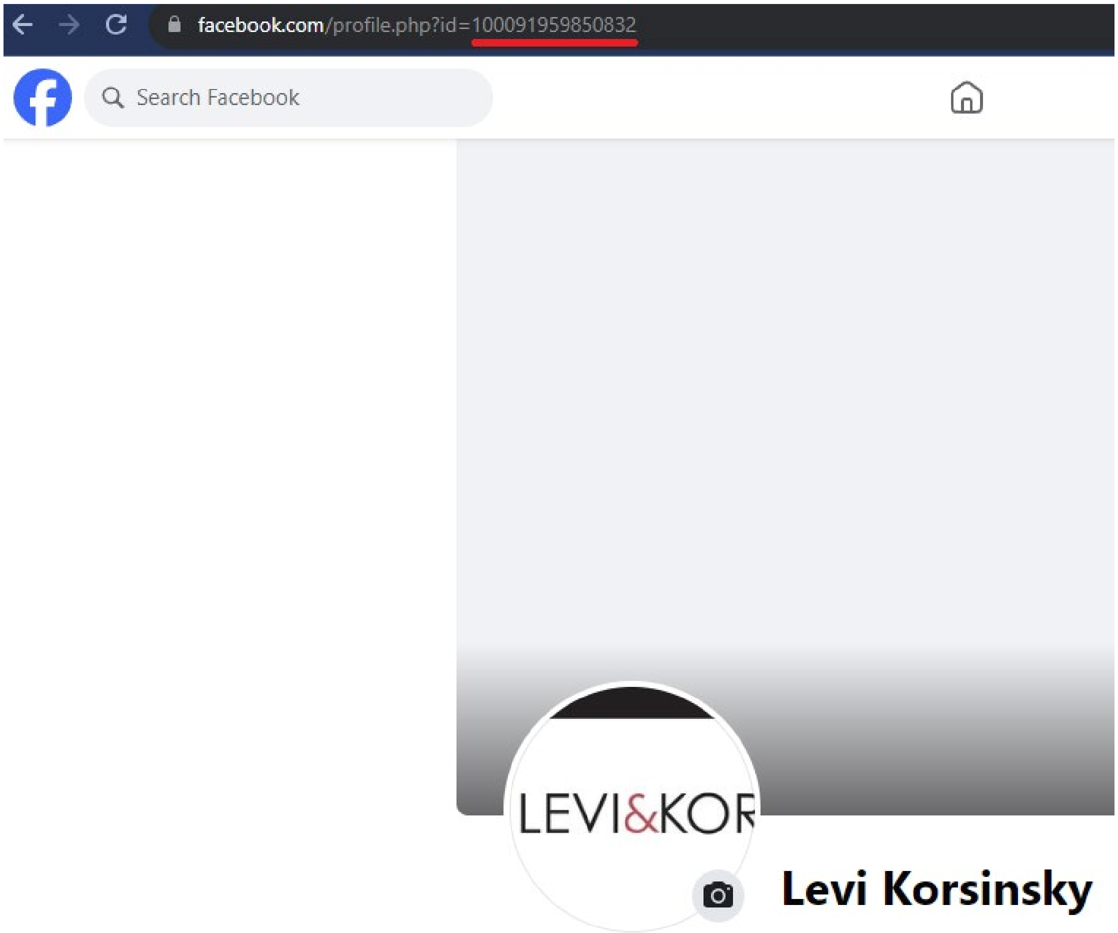


Figure 18- Appending UID of a user to "facebook.com/" results in the user being redirected to the user's profile

159. That step, readily available through any internet browser, will direct the browser to the profile page, and all the information contained in or associated with the profile page, for the user associated with that UID.

160. Importantly, some Facebook profile information – name, gender, profile photo, cover photo, username, user ID (account number), age range, language, and country – are "always public."[71] No privacy setting on a Facebook account would allow Plaintiff, or any users, to hide this basic information.

161. Defendant also uploads customer lists to Meta that contain Tracked Users' email addresses and purchase information, including what prescription eyewear they purchased or viewed. Defendant uploads these lists to Meta so that Meta can match Tracked Users to their Facebook profiles.

162. Meta admits that "[advertisers] provide us with information about [their] existing customers and we match this information with Facebook profiles."[72] The customer lists must contain "'identifier[s] (such as email, phone number, address)"[73] so that Meta can match the lists to "Facebook profiles" and "[advertisers] can advertise to [their] customers on Facebook, Instagram and Audience Network."[74]

163. Defendant also combines these customer lists with offline event data to effectively target Tracked Users. When advertisers create an ad campaign, Meta will "match the offline data [advertisers] upload to the event set so that [advertisers] can see how much [their] ads resulted in offline activity."[75] Meta also recommends that advertisers, like Defendant, provide an accurate timestamp for each event, down to "the minute or second."

[71] *Control who can see what you share on Facebook*, FACEBOOK, https://www.facebook.com/help/1297502253597210 (last visited October 31, 2024).

[72] *Create a Customer Audience List*, FACEBOOK, https://www.facebook.com/business/help/170456843145568?id=2469097953376494 (last visited October 31, 2024).

[73] *Id.*

[74] *Customer List Custom Audiences*, FACEBOOK, https://www.facebook.com/business/help/341425252616329?id=2469097953376494 (last visited October 31, 2024).

[75] *Upload Offline Event Data*, FACEBOOK, https://www.facebook.com/business/help/1554379615727700?id=565900110447546 (last visited October 31, 2024).

.

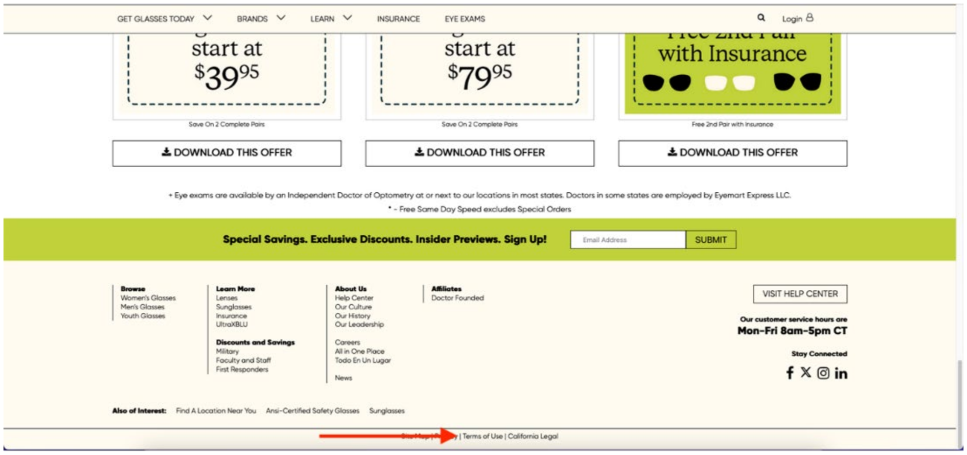
164. Defendant uploaded customer lists and offline events so it could match a Tracked Users' searches, purchases, and eye exam appointments with their corresponding Facebook profile.

G. Plaintiffs Did Not Consent to Defendant's Sharing of Plaintiffs' Website Activity

165. Plaintiffs and Class members were unaware of the tracking tools intercepting their confidential communications with the Website.

166. Plaintiffs and Class members reasonably believed that communications to the Website were made in confidence and that they would not be shared with third parties.

167. The actual terms of the Website are attached in a browsewrap format, with a hyperlink at the bottom of the page, which users must scroll to the very bottom of a large webpage to see, as depicted below:



+ Eye exams are available by an Independent Doctor of Optometry at or next to our locations in most states. Doctors in some states are employed by Eyemart Express LLC.

* - Free Same Day Speed excludes Special Orders

Our customer service hours are Mon-Fri 8am-5pm CT

Figure 19 – Terms of Use as found on the Website

168. While the Terms of Use only mention that the Website contains only "general information or content related to medical conditions, treatment, and other health care topics."[76]

[76] *Terms of Use*, EYEMART EXPRESS, https://eyemartexpress.com/pages/terms-of-use https://www.eyemartexpress.com/support/terms (last visited October 31, 2024).

169. Defendant's Privacy Policy apparently "does not apply to protected health information (as that term is defined in the Health Insurance Portability and Accountability act of 1996, or HIPAA) . . . ."[77] "Instead, [Defendant's] Notice of Privacy Practices applies to protected health information."[78] Defendant's Privacy Policy asserts that "most areas of the Site are not intended or designed to collect protected health information" though there are areas where PHI "is requested (such as when scheduling appointment)."[79]

170. However, no mention is made of Defendant's "Ecommerce Privacy Policy" in its Terms of Use or Privacy Policy.

171. Defendant's "Ecommerce Privacy Policy" directly admits that Defendant collects "consumer health data" as "defined by applicable laws in Nevada and Washington[.]"[80]

172. Defendant acknowledges that "using or accessing [Defendant's] Site" results in "the collection, use, and disclosure of [Tracked Users'] consumer health data[,]" including: (i) "[i]nformation about [Tracked Users'] health conditions, symptoms, status, diagnoses, testing, or treatments (including surgeries, procedures, medications, or other interventions)"; (ii) [i]nferences about [Tracked Users] "based on health-related goods and services purchased on the Site;" (iii) "[i]nformation that identifies a consumer seeking health care services;" and (iv) "[o]ther information that identifies your past and present health status[.]"[81]

173. Defendant also admits that it, and its vendors, "may use cookies and related technologies to passively collect information from and across your devices when you interact with our Site, our emails, or other online content."[82]

[77] *Privacy Policy*, EYEMART EXPRESS, https://eyemartexpress.com/pages/privacy-policy (last visited October 31, 2024).
[78] *Id.*
[79] *Id.*
[80] Ecommerce Privacy Policy, Eyemart Express, https://eyemartexpress.com/pages/ecommerce-privacy-policy (last visited October 31, 2024).
[81] *Id.*
[82] *Id.*

174. Defendant acknowledges that the purposes for collecting this information include: (i) conducting "research and analyses to enhance or improve [Defendant's] content, products, and services;" (ii) provide Tracked Users "with customized content or targeted offers; (iii) provide Tracked Users with "information, newsletters and promotional materials;" and (iv) create data "in an aggregated format that may be used for analytical and demographic purposes."[83]

175. Defendant also acknowledges its use of the Tracking Tools, noting that third parties "may be able to collect consumer health data from [Tracked Users] . . . ."[84]

176. However, Defendant's own Ecommerce Privacy Policy admits that Defendant "will obtain [Tracked Users'] consent or authorization where required by applicable law in connection with any of the uses described above." However, no such consent was requested or obtained.

177. Defendant's HIPAA Privacy Policy notes that Eyemart is "required by federal law to maintain the privacy of \health information that identifies [Tracked Users] or that could be used to identify [Tracked Users] . . . ."[85]

178. Specifically, Eyemart claims that it may disclose Tracked Users' PHI, without written authorization, "for certain routine uses and disclosures, such as those made for treatment, payment and the operation of our business."[86]

179. Eyemart claims that "[o]ther uses and disclosures of your PHI, not described [in the Notice of Privacy Practices], will be made only with [Tracked Users'] written authorization . . . ."[87]

[83] *Id.*

[84] *Id.*

[85] *Notice of Privacy Practices*, EYEMART EXPRESS, https://eyemartexpress.com/pages/notice-of-privacy-practices (last visited October 31, 2024).

[86] *Id.*

[87] *Id.*

180. Eyemart specifically notes that it must obtain users "written authorization to use and disclose [their] PHI for most marketing purposes."[88]

181. Meta also guides and cautions website operators of the dangers of using its tracking tools without first providing notice of and then obtaining valid consent for invasively collecting Plaintiffs' protected data and either making that data available to third-parties or allowing third parties to intercept Plaintiffs' protected information.[89]

182. Meta provides notice of its practices through its Business Tools Terms, which encompasses the Pixel, Conversions API, and other tools, and through tutorials it provides on how to use the Pixel. Eyemart agreed to these terms, directly or as the effective owner of the Website, in order to utilize and employ the tracking tools.[90]

183. Meta is clear that while Conversions API collects information through a web developers' servers, the Pixel is used to collect information from users' browsers.[91]

184. Meta's Business Tools Terms, which a website must accept before making use of the Pixel, are clear that the Pixel will intercept, collect, and transmit two categories of data: (i) "Contact Information" which "personally identifies individuals, such as names, email addresses, and phone numbers" which are used "for matching purposes[;]" and (ii) "Event Data" that reveals information about "people and the actions that they take on your websites and apps . . . such as visits to your sites . . . and purchases of your products" (collectively Business Tool Data).[92]

[88] *Id.*
[89] *Meta Business Tools Terms*, FACEBOOK (Section 3(c)(i)) https://www.facebook.com/legal/businesstech?paipv=0&eav=AfY375fgb725ZjQrZEqZyhoJsO63s7_tFmEPfgnFpew1xw5Wldq7ONw04KTB0G0o-i4&_rdr (last visited October 31, 2024).
[90] *Id.* (conditioning use of the Pixel on acceptance of Meta's Business Tools Terms).
[91] *Meta for Developers: Conversions API End-to-End Implementation*, FACEBOOK, https://developers.facebook.com/docs/marketing-api/conversions-api/guides/end-to-end-implementation/ (last visited October 31, 2024).
[92] *Meta Business Tools Terms*, FACEBOOK (Section 1(a)(i)), https://www.facebook.com/legal/businesstech?paipv=0&eav=AfY375fgb725ZjQrZEqZyhoJsO63s7_tFmEPfgnFpew1xw5Wldq7ONw04KTB0G0o-i4&_rdr (last visited October 31, 2024).

185. Meta's Business Tools Terms also highlight that Meta "will not share Business Tool Data provided by a website, including advertisers, unless the website developers opt-in to Facebooks advertising programs or disclosure is mandated by law.[93] In short, Eyemart must have opted-in to Meta's data sharing program for advertising purposes.

186. Meta is also clear in its Business Tools Terms that once they receive Business Tool Data from a website developer, like Eyemart, Meta will "process the Contact Information . . . to match the Contact Information against user IDs . . . as well as to combine those user IDs with corresponding Event Data."[94]

187. Meta's terms warn that website developers must not "share Business Tool Data with [Meta] that you know or reasonably should know . . . includes health . . . information or other categories of sensitive information[.]"[95]

188. In contravention to Meta's terms and guidance, Defendant collected Plaintiffs' PHI and Plaintiffs were not given notice of the use of the tracking tools on the Website, including Meta's Pixel.

189. As a result, Plaintiffs did not and could not provide consent to the collection and sharing of their data when communicating Queries to the Website, viewing, or attempting to schedule eye exams.

TOLLING

190. The statutes of limitations applicable to Plaintiffs' and the Classes' claims were tolled by Eyemart's conduct and Plaintiffs' and Class Members' delayed discovery of their claims.

191. As alleged above, Plaintiffs and members of the Classes did not know and could not have known when they used the Website that Eyemart was disclosing their information and

[93] *Id.* at Section 1(b)
[94] *Id.* at Section 2(a)(i).
[95] *Id.* at Section 1(h)

communications to third parties. Plaintiffs and members of the Classes could not have discovered Eyemart's unlawful conduct with reasonable diligence.

192. Eyemart secretly incorporated the Tracking Entity' tracking tools into the Website, providing no indication to Tracked Users that their communications would be disclosed to these third parties.

193. Eyemart had exclusive and superior knowledge that the Tracking Entity' tracking tools incorporated on its Website would disclose Tracked Users' protected and private information and confidential communications, yet failed to disclose to Tracked Users that by interacting with the Website that Plaintiffs' and Class Members' Queries, PHI, and website interactions would be disclosed to third parties.

194. Plaintiffs and Members of the Classes could not with due diligence have discovered the full scope of Eyemart's conduct because the incorporation of the Tracking Entity' tracking tools is highly technical and there were no disclosures or other indication that would inform a reasonable consumer that Eyemart was disclosing and allowing the interception of such information to these third parties.

195. The earliest Plaintiffs and Class Members could have known about Eyemart's conduct was in connection with their investigation and the work done on their behalf in preparation of filing of this Complaint.

CLASS ACTION ALLEGATIONS

196. Plaintiffs bring this action individually and on behalf of the following Classes:

197. Nationwide Class of Tracked Users: All persons in the United States whose searches and activity on the Website were intercepted, stored, and shared through the use of tracking tools (the "Class" or "Nationwide Class").

198. Missouri Subclass of Tracked Users: All persons in Missouri whose searches and activity on the Website were intercepted, stored, and shared through the use of tracking tools (the "Missouri Class").

> Illinois Subclass of Tracked Users: All persons residing in Illinois whose searches and activity on Website were intercepted, stored, and shared through the use of tracking tools (the "Illinois Class").

199. Specifically excluded from the Classes are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

200. Plaintiffs reserve the right to amend the Class definitions above if further investigation and/or discovery reveals that the Classes should be expanded, narrowed, divided into additional subclasses, or otherwise modified in any way.

201. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

202. Numerosity (Rule 23(a)(1)): At this time, Plaintiffs do not know the exact number of members of the aforementioned Class. However, given the popularity of Eyemart's Website,

the number of persons within the Class is believed to be so numerous that joinder of all members is impractical.

203. Typicality of Claims (Rule 23(a)(3)): Plaintiffs' claims are typical of those of the Class because Plaintiffs, like all members of the Class, visited the Website and searched for medical- or otherwise sensitive health-related products, added the items to their cart and/or purchased the items on the Website. Plaintiffs' and Class members' PHI was then disclosed and shared by Eyemart to third parties.

204. Adequacy of Representation (Rule 23(a)(4)): Plaintiffs will fairly and adequately represent and protect the interests of the Class. Plaintiffs have no interests antagonistic to, nor in conflict with, the Class. Plaintiffs have retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

205. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members is relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

206. Commonality and Predominance (Rule 23(a)(2), 23(b)(3)): There is a well-defined community of interest in the questions of law and fact involved in this case. Questions of law and fact common to the members of the Class that predominate over questions that may affect individual members of the Class include:

a. Whether Eyemart implemented the Tracking Entity' tools on the Website;

b. Whether the Tracking Entity collected Plaintiffs' and the Class's PHI, Queries, and webpage interactions on the Website;

c. Whether Eyemart's disclosures of Plaintiffs' and Class Members' PHI was without consent or authorization;

d. Whether Eyemart unlawfully disclosed and continue to disclose the PHI, Queries, and webpage interactions of Tracked Users;

e. Whether Eyemart's omissions regarding the practices alleged herein constitute an unfair and/or deceptive practice; and

f. Whether Eyemart's disclosures were committed knowingly.

207. Information concerning Eyemart's Website data sharing practices is available from Eyemart's or third-party records.

208. Plaintiffs know of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

209. The prosecution of separate actions by individual members of the Classes would run the risk of inconsistent or varying adjudications, and establish incompatible standards of conduct for Eyemart. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

210. Eyemart has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

211. Eyemart has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

212. Given that Eyemart's conduct is ongoing, monetary damages are insufficient and there is no complete and adequate remedy at law.

COUNT I

VIOLATION OF THE FEDERAL WIRETAP ACT
18 U.S.C. § 2510, et. seq.
(On Behalf of Plaintiffs and the Nationwide Class)

213. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in paragraphs 1 through 25 and paragraphs 35 through 195 as though fully set forth herein.

214. Plaintiffs bring this claim individually and on behalf of the members of the proposed class against Facebook and Eyemart.

215. Codified under 18 U.S.C. U.S.C. §§ 2510 et seq., the Federal Wiretap Act (the "Wiretap Act") prohibits the interception of any wire, oral, or electronic communications without the consent of at least one authorized party to the communication.

216. The Wiretap Act confers a civil private right of action to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

217. The Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

218. The Wiretap Act defines "contents" as "includ[ing] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

219. The Wiretap Act defines "person" as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6).

220. The Wiretap Act defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part

by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce . . . .” 18 U.S.C. § 2510(12).

221. Eyemart is a person under the Wiretap Act.

222. The Pixel constitutes a “device or apparatus which can be used to intercept a wire, oral, or electronic communication.” 18 U.S.C. § 2510(5).

223. The confidential communications between Plaintiffs and the Nationwide Class and the Website, in the form of their PHI were intercepted by Eyemart and Meta, utilizing Meta’s Pixel, and such communications were “electronic communications” under 18 U.S.C. § 2510(12).

224. The Wiretap Act is applicable to both the sending and receipt of communications.

225. Plaintiffs and the Nationwide Class had a reasonable expectation of privacy in their electronic communications with the Website in the form of their PHI. Interception of Plaintiffs’ and Nationwide Class Members’ communications with the Website occurs in the regular course of using the Website, whether the Tracked Users look for a location to schedule eye exam appointments, search for prescription products on the Website, purchase prescription products on the Website, or look for a physical location to purchase prescription eyewear. Moreover, Meta is not a party to these communications.

226. Eyemart violated the Wiretap Act by using Meta and its Pixel to intercept Plaintiffs’ communications with Eyemart, and for utilizing the communications that Meta intercepted and analyzed for advertising purposes. 18 U.S.C. § 2511(1)(a)-(c).

227. The interception and use of Plaintiffs’ and Nationwide Class Members’ communications with their health care provider, Eyemart, was intentional and knowing as indicated by: (a) Eyemart’s choice to use the Pixel on its Website; (b) Eyemart’s knowledge that utilizing Pixel on the Website would allow Meta to link user activity and user identities, allowing

Meta to create targetable audiences; and (c) Eyemart's failure to prevent sensitive health information from being transmitted to Meta using the Pixel.

228. Eyemart's use of the Pixel to intercept these communications resulted in Plaintiffs' and Class Members' communications with Eyemart to be duplicated and sent to Meta the instant the Pixel Events were triggered.

229. The intercepted communications, in the form of PHI, between Plaintiffs, the Nationwide Class Members, and the Website constitute the "contents" of the communications for purposes of the Wiretap Act.

230. Eyemart did not receive consent from Plaintiffs or the Nationwide Class before it used the Pixel to intercept and disclose their PHI to Meta, and subsequently used their sensitive PHI for advertising purposes. Indeed, such consent could not have been given as Eyemart never sought any form of consent from Plaintiffs or the Nationwide Class to intercept, record, and disclose their private communications with the Website, and explicitly claimed it would not use PHI for such purposes.

231. As detailed above, Eyemart's unauthorized interception, disclosure and use of Plaintiffs' and the Nationwide Class Members' PHI was only possible through its knowing, willful, or intentional placement of Pixel on the Website. 18 U.S. Code § 2511(1)(a).

232. Eyemart's use of the Pixel to intercept Plaintiffs' and Class Members' communications was done for purposes of committing criminal and tortious acts in violation of the laws of the United States, including criminal violation of HIPAA, 42 U.S.C. § 1320d-6.

233. Under 42 U.S.C. § 1320d-6, it is a criminal violation for a person to "use[] or cause[] to be used a unique health identifier" or to "disclose[] individually identifiable health information to another person … without authorization" from the patient.

234. Under the statute, "individually identifiable health information" (IIHI) is defined as "any information, including demographic information collected from an individual, that—(A) is created or received by a healthcare provider …; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual, and (i) identifies the individual, or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual." 42 U.S.C. § 1320d(6).

235. Thus, under the plain language of the statute, IIHI includes "any information …. that … relates to … the provision of healthcare to an individual" and either identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. The clause relating to "the provision of healthcare to an individual" covers patient-status because the fact that someone is a patient of a specific provider is information relating to the fact that the specific healthcare provider provides healthcare to the individual.

236. The information at issue in this case fits the "provision of healthcare to an individual" element because it includes patient-status when Eyemart discloses patients' attempts to schedule a doctor visit or specific medical care facility.

237. The information at issue in this case also fits the "relates to the past, present, or future physical or mental health or condition of an individual" because the information disclosed related to the Plaintiffs' doctors.

238. The information at-issue in this case fits the elements for identifiability because it includes URLs, the c_user cookie (and the FID contained therein), and other information that fits under the list of identifiers in the HIPAA de-identification rule (rendering them "identifiable" as a matter of law) and that are identifiable as a matter of fact.

239. Eyemart's conduct violated 42 U.S.C. § 1320d-6 in that it:

a) Used and caused to be used c_user cookies associated with specific patients without patient authorization; and

b) Disclosed individually identifiable health information to, at a minimum, Meta.

240. Eyemart's conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Eyemart's use of the Pixel was for Eyemart's commercial advantage to increase revenue from existing patients and gain new patients.

241. Plaintiffs and the Nationwide Class have been damaged due to the unauthorized interception, disclosure, and use of their confidential communications in violation of 18 U.S.C. § 2520. As such, Plaintiffs and the Nationwide Class are entitled to: (1) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and the Nationwide Class and any profits made by Eyemart as a result of the violation, or (b) statutory damages of whichever is the greater of $100 per day per violation or $10,000; and (2) appropriate equitable or declaratory relief; (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT II

VIOLATION OF THE MISSOURI WIRETAP ACT
R.S. Mo. § 542.400, *et seq*
(On Behalf of Plaintiff Rand and the Missouri Class)

242. Plaintiff Rand incorporates by reference and re-allege each and every allegation set forth above in paragraphs 1 through 25 and paragraphs 35 through 195 as though fully set forth herein.

243. Plaintiff Rand brings this claim individually and on behalf of the members of the proposed Missouri Class against Eyemart.

244. The Missouri Wiretap Act prohibits provides a civil cause of action "against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or

use" a "person['s]" wire communications that are "intercepted, disclosed, or used in violation of sections 542.400 to 542.422 . . . ." R.S. Mo. § 542.418.2(1).

245. Eyemart and Plaintiff Rand qualify "person[s]" as defined by R.S. Mo. § 542.400.9.

246. Electronic communications between Plaintiff Rand and the Website qualify as "wire communications" pursuant to R.S. Mo. § 542.400.12. See *Phillips v. American Motorist Ins. Co*., 996 S.W.2d 584, 591 (Mo. App. W.D. 1999).

247. Eyemart procured Meta to "intercept" Plaintiff Rand and Missouri Class Members' communications with Eyemart, in violation of the Missouri Wiretap Act, which defines "intercept" as "[a]ural acquisition of the contents of any wire communication through the use of any electronic or mechanical device . . . ." R.S. Mo. § 542.400.6.

248. Meta's Pixel qualifies as an "electronic[] device," which is defined by the Missouri Wiretap Act as including "any device or apparatus which can be used to intercept a wire communication . . . ." R.S. Mo. § 542.400.5

249. Eyemart subsequently used the contents of Plaintiff Rand's communications with Eyemart, intercepted and processed by Meta, to target users with advertising, which is prohibited under the Missouri Wiretap Act. R.S. Mo. § 542.418.2(1).

250. Defendant aided in the interception of communications between Plaintiff Rand and Missouri Class Members and Defendant that were redirected to and recorded by third parties without the Plaintiff Rand or Missouri Class Members' consent.

251. Plaintiff Rand and the Missouri Class Members are patients of Eyemart and need access to Eyemart's Website (www.Eyemart.com), in connection with receiving health care from Eyemart. Because Plaintiff Rand and Missouri Class members need to, and so will continue to use Eyemart's Website in the future, if Eyemart's unfair, unlawful, and deceptive trade practices are

allowed to continue, Plaintiff Rand and Missouri Class members are likely to suffer continuing harm in the future.

252. Plaintiff Rand and members of the Missouri Class Members seek all relief available for violations of the Missouri Wiretap Act, including recovery of actual damages that are not less than liquidated damages computed at a rate of $100.00 a day for each day of violation or $10,000.00, whichever is higher; punitive damages for willful or intentional violations; and reasonable attorneys' fees and other litigation costs reasonably incurred, along with injunctive relief. R.S. Mo. § 542.418.2(2).

COUNT III

VIOLATION OF THE ILLINOIS EAVESDROPPING ACT
720 ILCS § 5/14-1, *et seq.*
(On Behalf of Plaintiff Soto and the Illinois Class)

253. Plaintiff Soto incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 25 and paragraphs 35 through 195 as though fully set forth herein.

254. Plaintiff Soto brings this claim individually and on behalf of the Illinois Class.

255. The Illinois Eavesdropping Statute ("IES"), 720 ILCS § 5/14-1, *et seq*., prohibits the surreptitious interception, recording, or transcription of private electronic communications without the consent of all parties to the conversation and provides a civil cause of action to a person subjected to a violation of the IES against eavesdroppers and their principals.

256. The IES makes it unlawful for a person to knowingly and intentionally intercept, record, or transcribe, in a surreptitious manner, any private electronic communication to which that person is not a party unless that person obtains consent of all parties to the private electronic communication. 720 ILCS § 5/14-2(a)(3).

257. 720 ILCS § 5/14-2(a)(5) of the IES makes it unlawful for a person to knowingly and intentionally use or disclose any information which that person knows, or reasonably should know, was obtained from a private conversation or private electronic communication in violation of the IES: a violation occurs unless that person does so with the consent of all of the parties.

258. The IES also makes it unlawful for a person to knowingly and intentionally "possesses any electronic, mechanical, eavesdropping, or other device knowing that or having reason to know that the design of the device renders it primarily useful for the purpose of the surreptitious overhearing, transmitting, or recording of private conversations or the interception, or transcription of private electronic communications and the intended or actual use of the device is contrary to the provisions of" the IES. 720 ILCS § 5/14-2(a)(4),

259. Under the IES, a "private electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation." 720 ILCS § 5/14-1(e). The data gathered by the Tracking Entity wasn't exclusively for the Website's advantage.

260. As used in the IES, "surreptitious," means "obtained or made by stealth or deception, or executed through secrecy or concealment." 720 ILCS § 5/14-1(g).

261. As used in the IES "eavesdropper" means "any person…who operates or participates in the operation of any eavesdropping device contrary to the provisions of [the IES] or who acts as a principal[.]" 720 ILCS § 5/14-1(b).

262. As outlined in 720 ILCS § 5/14-1(c), a "principal" includes any person who "[k]nowingly derives any benefit or information from the illegal use of an eavesdropping device by another" or "[d]irects another to use an eavesdropping device illegally on his or her behalf."

263. As used in 720 ILCS § 5/14-1(a)., an “eavesdropping device” is “any device capable of being used to…intercept…electronic communications[.]”

264. Plaintiff Soto’s communications with Eyemart constituted private electronic communications. Plaintiff transmitted his communications to Eyemart from their computers or by wire, intended the communications to be private, and reasonably expected the communications to be private under HIPAA, Eyemart’s express promises of confidentiality, the physician-patient relationship, and other State and federal laws protecting the confidentiality of Plaintiff’s communications.

265. Facebook was not a party to Plaintiff Soto’s private electronic communications with Eyemart. Plaintiff believed he was only communicating with Eyemart, intended for their communications to be directed at Eyemart only, and were unaware of the presence of concealed source code that redirected their communications.

266. Facebook knowingly, intentionally, and covertly intercepted the private electronic communications of the Plaintiff Soto. Facebook deliberately structured its source code to hide within websites, enabling the clandestine interception of private communications. Based on gathered information and belief, Facebook was aware that its source code possessed the capability to intercept private electronic communications without the consent of all parties involved.

267. Facebook used and disclosed Plaintiff Soto’s intercepted communications for advertising purposes.

268. Facebook’s conduct was done without Plaintiff Soto’s consent, in violation of 720 ILCS § 5/14-2(a)(3) and (a)(5).

269. Eyemart functioned as Facebook's "principal" according to the IES. Through the utilization of Facebook's source code on its online platforms, Eyemart instructed Facebook to unlawfully eavesdrop on the private electronic communications of the Plaintiff Soto on its behalf.

Eyemart, with awareness, gained advantages and insights from the illegal eavesdropping, particularly in the realm of marketing.

270. Eyemart violated 720 ILCS § 5/14-2(a)(4) by possessing the source code, knowing that its design rendered it primarily useful for surreptitiously intercepting private electronic communications contrary to the IES.

271. Eyemart's violation of the IES was wanton, reckless, and/or malicious.

272. For Eyemart's violations of the IES, Plaintiff Soto and Class members seek actual damages, punitive damages, injunctive relief, and any other relief the Court deems just.

COUNT IV

INTRUSION UPON SECLUSION
(On Behalf of Plaintiffs and the Nationwide Class)

273. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in paragraphs 1 through 25 and paragraphs 35 through 195 as though fully set forth herein.

274. Plaintiffs bring this claim individually and on behalf of the members of the proposed Classes against Eyemart.

275. Eyemart intentionally intruded upon class members' solicitude or seclusion in that it effectively placed Meta in the middle of conversations including PHI to which it was not an authorized party.

276. Eyemart's participation in Meta's tracking and interception of PHI were not authorized by Plaintiffs or Class members.

277. Eyemart's enabling of Meta's intentional intrusion into Plaintiffs' and Class members' internet communications including PHI and their computing devices and web-browsers was highly offensive to a reasonable person in that they violated federal and state criminal and civil laws designed to protect individuals against privacy and against theft.

278. Secret monitoring of PHI is highly offensive behavior.

279. Wiretapping and the surreptitious recording of communications including PHI is highly offensive behavior.

280. Public polling on internet tracking has consistently revealed that the overwhelming majority of Americans believe it is important or very important to be "in control of who can get information" about them; to not be tracked without their consent; and to be in "control[] of what information is collected about [them]." The desire to control one's information is only heightened while a person is handling PHI. Plaintiffs and Class members have been damaged by Eyemart ' facilitation of Meta's intrusion upon their seclusion and are entitled to reasonable compensation including but not limited to disgorgement of profits related to the unlawful internet tracking.

COUNT V

BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

281. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in paragraphs 1 through 25 and paragraphs 35 through 195 as though fully set forth herein.

282. Plaintiffs bring this claim individually and on behalf of the members of the proposed Classes against Eyemart.

283. When Plaintiffs and Class Members provided their PHI to Eyemart, they entered into an implied contract pursuant to which Eyemart agreed to safeguard and not disclose their PHI without consent.

284. Plaintiffs and Class Members would not have entrusted Eyemart with their PHI in the absence of an implied contract between them and Eyemart obligating Eyemart to not disclose PHI without consent.

285. Plaintiffs and Class Members would not have used the Website in the absence of an implied contract between them and Eyemart obligating Eyemart to not disclose PHI without consent.

286. Eyemart breached these implied contracts by disclosing Plaintiffs' and Class Members' PHI without consent to third parties like Facebook.

287. As a direct and proximate result of Eyemart's breaches of these implied contracts, Plaintiff and Class Members sustained damages as alleged herein, including but not limited to the loss of the benefit of their bargain and diminution in value of PHI.

288. Plaintiffs and Class Members are entitled to compensatory and consequential damages as a result of Eyemart's breach of implied contract.

COUNT VI

BREACH OF CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

289. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in paragraphs 1 through 25 and paragraphs 35 through 195 as though fully set forth herein.

290. Plaintiffs bring this claim individually and on behalf of the members of the proposed Classes against Eyemart.

291. When Plaintiffs and Class Members provided their PHI to Eyemart, they entered into an express contract pursuant to which Eyemart, in the form of Eyemart's Terms of Use on the Website. That contract included the promise to protect nonpublic personal information given to Eyemart or that Eyemart gathered on its own, from disclosure.

292. Eyemart breached its contractual obligations to protect the nonpublic personal information it possessed and was entrusted with when the information was disclosed to third-parties, absent consent.

293. Plaintiffs and Class Members would not have entrusted Eyemart with their PHI in the absence of an express contract between them and Eyemart obligating Eyemart to not disclose PHI without consent.

294. Plaintiffs and Class Members would not have used the Website in the absence of an express contract between them and Eyemart obligating Eyemart to not disclose PHI without consent.

295. Eyemart breached these express contracts by disclosing Plaintiffs' and Class Members' PHI without consent to third parties like Facebook.

296. As a direct and proximate result of Eyemart's breaches of these contracts, Plaintiff and Class Members sustained damages as alleged herein, including but not limited to the loss of the benefit of their bargain and diminution in value of PHI.

297. Plaintiffs and Class Members are entitled to compensatory and consequential damages as a result of Eyemart's breach of contract.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek judgment against Eyemart, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiffs as the representatives of the Classes and their counsel as Class Counsel;

(b) For an order declaring that the Eyemart' conduct violates the statutes referenced herein;

(c) For an order finding in favor of Plaintiffs and the Classes on all counts asserted herein;

(d) Entry of an order for injunctive and declaratory relief as described herein, including, but not limited to, requiring Eyemart to immediately (i) remove the tracking tools from the Website or (ii) add, and obtain, the appropriate consent from Tracked Users;

(e) For damages in amounts to be determined by the Court and/or jury;

(f) An award of statutory damages or penalties to the extent available;

(g) For pre-judgment interest on all amounts awarded;

(h) For an order of restitution and all other forms of monetary relief;

(i) An award of all reasonable attorneys' fees and costs; and

(j) Such other and further relief as the Court deems necessary and appropriate.

DEMAND FOR TRIAL BY JURY

Plaintiffs demand a trial by jury of all issues so triable.

Dated: October 31, 2024

FOSTER YARBOROUGH PLLC

By: */s/ Patrick Yarborough*
Patrick Yarborough
Marshal J. Hoda*
Jeffrey Lucas Ott
917 Franklin Street, Suite 220
Houston, TX 77002
Telephone: (713) 331-5254
Facsimile: (713) 513-5202
Email: patrick@fosteryarborough.com
Email: marshal@fosteryarborough.com
Email: luke@fosteryarborough.com

LEVI & KORSINSKY, LLP

Mark S. Reich*
Courtney Maccarone*
Gary S. Ishimoto (*pro hac vice*)*
33 Whitehall Street, 17th Floor
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: mreich@zlk.com
Email: cmaccarone@zlk.com
Email: gishimoto@zlk.com

Counsel for Plaintiffs

**pro hac vice* forthcoming